www.mruni.eu

Deividas KIRŠYS

DAKTARO DISERTACIJA

KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS

SOCIALINIAI MOKSLAI,
TEISĖ (S 001)
VILNIUS, 2025

M R U
Mykolo Romerio
universitetas

MYKOLO ROMERIO UNIVERSITETAS

Deividas Kiršys

KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS

Mokslo daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Vilnius, 2025

Mokslo daktaro disertacija rengta 2017–2024 m. Mykolo Romerio universitete pagal Mykolo Romerio universitetui su Vytauto Didžiojo universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 „Dėl doktorantūros teisės suteikimo“ suteiktą doktorantūros teisę.

Mokslinė vadovė:
prof. dr. Simona Drukteinienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Mokslo daktaro disertacija ginama Mykolo Romerio universiteto ir Vytauto Didžiojo universiteto teisės mokslo krypties taryboje:

Pirmininkė:
prof. dr. Salvija Mulevičienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Nariai:
doc. dr. Remigijus Jokubauskas (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001);
prof. dr. Jurgita Malinauskaitė (Londono Brunelio universitetas, Jungtinė Karalystė, socialiniai mokslai, teisė, S 001);
prof. dr. Lina Mikalonienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001);
doc. dr. Saulė Milčiuvienė (Vytauto Didžiojo universitetas, socialiniai mokslai, teisė, S 001).

Mokslo daktaro disertacija ginama viešame Teisės mokslo krypties tarybos posėdyje 2025 m. balandžio 28 d. 13:00 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, 08303 Vilnius.

TURINYS

SANTRUMPOS IR SUTRUMPINIMAI

a. – amžius
angl. – anglų kalba
ANK – Lietuvos Respublikos administracinių nusižengimų kodeksas
APEC (angl. *Asia-Pacific Economic Cooperation*) – Azijos ir Ramiojo vandenyno šalių ekonominis bendradarbiavimas
ATM (angl. *Air Traffic Management*) – oro eismo valdymas
aut. vert. – autoriaus vertimas
BDAR – Bendrasis duomenų apsaugos reglamentas (2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinta Direktyva 95/46/EB)
Bepilotis orlaivis – žr. disertacijos 1.1 poskyrį. Disertaciniame darbe atliekama analizė apsiriboja bepiločiais orlaiviais, naudojamais komerciniais tikslais, ir neįtraukia kariniais, viešojo saugumo tikslais naudojamų skraidyklių.
BK – Lietuvos Respublikos baudžiamasis kodeksas
BVLOS (angl. *Beyond visual line of sight*) – bepiločio orlaivio skrydis, kurio metu skraidomoji bepiločio dalis nėra aiškiai matoma
CCTV (angl. *Closed Circuit Television*) – technine prasme gali būti suprantama dvejopai: pirma, kaip kabelinė televizija, antra, kaip skaitmeninė vaizdo stebėjimo sistema. Šiame darbe ji suprantama išimtinai kaip skaitmeninė vaizdo stebėjimo sistema
CFR (angl. *Code of Federal Regulations*) – JAV Federalinių teisės aktų kodeksas
CK – Lietuvos Respublikos civilinis kodeksas
DG29 – pagal Europos Sąjungos 95/46/EB direktyvos 29 straipsnį sukurta darbo grupė, kuri užtikrintų asmenų apsaugą tvarkant jų duomenis; įsigaliojus BDAR ją pakeitė analogiškas funkcijas atliekanti EDAV
EASA (angl. *European Union Aviation Safety Agency*) – Europos aviacijos saugumo agentūra, atsakinga už aviacijos saugumą ES
EBPO – Ekonominio bendradarbiavimo ir plėtros organizacija
EDAV – Europos duomenų apsaugos valdyba
ES – Europos Sąjunga
ESTT – Europos Sąjungos Teisingumo Teismas
EŽTK – Europos Žmogaus Teisių Konvencija
EŽTT – Europos Žmogaus Teisių Teismas

---

1 Raimundas Kalesnykas ir Vidmantas Mečkauskas, „Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą: teisiniai ir organizaciniai aspektai“, *Jurisprudencija* 36, 28 (2002): 59–70.

FAA (angl. *Federal Aviation Administration*) – Federalinė aviacijos administracija (JAV)
ICAO (angl. *International Civil Aviation Organization*) – Tarptautinė civilinės aviacijos organizacija
infra – disertacijos išnašose vartojama santrumpa, reiškianti – toliau einanti dalis
JARUS (angl. *Joint Authorities for Rulemaking on Unmanned Systems*) – ekspertų grupė, sudaryta iš įvairių pasaulio šalių ekspertų ir nacionalinės valdžios institucijų, kurios tikslas – sukurti bepiločių orlaivių reglamentavimo standartus ir teikti rekomendacijas, kaip palengvinti nacionalinių bepiločių orlaivių teisės aktų kūrimą
JAV – Jungtinės Amerikos Valstijos
JK – Jungtinė Karalystė
Kasacinis teismas – Lietuvos Aukščiausiasis Teismas
LAT – Lietuvos Aukščiausiasis Teismas
LR – Lietuvos Respublika
LUC – lengvosios UAS naudotojų pažymėjimas. Tai dokumentas, patvirtinantis, jog bepiločio orlaivio valdytojas gali pats įvertinti operacijos riziką ir vykdyti tam tikrus ar visus skrydžius civilinės aviacijos organizacijai neteikdamas atskiros deklaracijos ar be atskiro civilinės aviacijos organizacijos leidimo. Norėdamas gauti LUC, bepiločio orlaivio valdytojas nacionalinės aviacijos organizacijai privalo įrodyti, kad atitinka reikalavimus, apibrėžtus Reglamento (ES) 2019/947 C dalyje
m. – metai
m – metras (-ai)
mlrd. – milijardai
NTIA (angl. *National Telecommunications and Information Administration*) – Nacionalinės telekomunikacijų ir informacijos administracija (JAV)
PDAV – poveikio duomenų apsaugai vertinimas
SESAR JU (angl. *SESAR Joint Undertaking*) – bendras viešojo ir privataus sektorių projektas ES mastu, kurio tikslas – sukurti naujovišką, automatizuotą ATM sistemą, į kurią būtų įtraukti ir bepiločiai orlaiviai
VDAI – Lietuvos Respublikos valstybinė duomenų apsaugos inspekcija
VLOS – skrydis, kuris vykdomas naudojant bepilotį orlaivį, kai nuotolinis pilotas nuolat be pagalbinių priemonių gali matyti bepilotį orlaivį ir valdyti jo skrydžio trajektoriją kitų orlaivių, žmonių ir kliūčių atžvilgiu, kad išvengtų susidūrimų
UAS (angl. *Unmanned Aerial System arba Unmanned Aircraft Systems*) – bepiločio orlaivio sistema, susidedanti iš skraidančio komponento bei palaikančių komponentų, tokių kaip valdymo pultas, navigacijos įranga, kliūčių vengimo įranga ir pan.

UTM (angl. *Unmanned Aircraft Systems Traffic Management*) – oro eismo valdymo rūšis, skirta bepiločių orlaivių oro eismui valdyti

v. – *versus*

ĮVADAS

Tyrimo aktualumas ir problematika. Šiuo metu pasaulis išgyvena virsmo laikotarpį, kai beveik kasdien išrandamos technologinės inovacijos, prie kurių reikia greitai prisitaikyti. Pasak profesoriaus Klauso Schwabo, dabar pokyčiai ekonominiame, socialiniame, kultūriniame šiuolaikinės visuomenės gyvenime yra tokie dideli, jog žmonijos istorijoje dar nebuvo tiek daug žadančio, bet ir tiek pavojų keliančio laikotarpio. Šis periodas yra ketvirtosios pramonės revoliucijos pradžia, kuri keičia ne tik kaip mes gyvename, bet ir kas mes esame[2].

Dažnai teigiama, kad teisė nespėja su technologiniais pokyčiais. Vieni tai vadina tempo problema (angl. the pacing problem[3]), kiti teisinio reguliavimo ryšio iššūkiu (angl. challenge of regulatory connection[4]), treti lygina su amžinomis lenktynėmis tarp vėžlio ir kiškio, kur teisė atlieka vėžlio, o technologijos – kiškio vaidmenį[5]. Nors teisė tarsi atsilieka nuo technologinių pokyčių, tačiau nuo jų visiškai neatitrūksta, nes inovacijos negali tobulėti be naujų elgesio standartų, o įstatymų leidėjai negali sukurti naujų elgesio standartų be realaus suvokimo, kaip naujas išradimas pakeis socioekonominius santykius.

Teisės aktų pakeitimai nustato naujas elgesio taisykles ir pakeičia ribas to, kas yra priimtina visuomenėje. Taip teisė veikia technologijų vystymąsi. Iš kitos pusės, technologiniai pokyčiai veikia žmonių socialinius ir politinius santykius, keičia atskirų socialinių grupių galios pusiausvyrą, todėl atsiranda naujo teisinio reguliavimo poreikis. Pvz., gali būti nebeaišku, kaip galiojančias taisykles taikyti produktui, paslaugai ar santykiui arba kaip jose klasifikuoti produktą, paslaugą ar santykį. Gali nutikti ir taip, kad galiojančios taisyklės reguliuoja elgesį, kuris tapo nebesvarbus, arba jos buvo sukurtos konkrečiam tikslui pasiekti, bet šis prarado aktualumą ar tapo per brangus įgyvendinti, palyginti su pigesnėmis alternatyvomis[6].

Nors per kelis pastaruosius dešimtmečius žmonių gyvenimus keitė daugybė technologijų, tik kelios jų paskatino peržiūrėti galiojančius teisės aktus. Mokslininkai aktyviai diskutuoja teisiniais klausimais, kylančiais dėl dirbtinio intelekto, biotechnologijos, kriptovaliutos, bet nekreipia dėmesio, kad būtina sureguliuoti, pvz., bevielių ausinių naudojimą. Daugumai naujų technologijų pakanka ir esamo teisinio reglamentavimo, kurį užtikrina bendri gamintojų

---

2 Klaus Schwab, *The fourth industrial revolution* (New York: Crown Business, 2017), 1–5.

3 Gary E. Marchant, Braden R. Allenby ir Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Dordrecht Heidelberg London New York: Springer Science & Business Media, 2011).

4 Roger Brownsword, *Rights, Regulation and the Technological Revolution* (New York: Oxford University Press, Inc., 2008).

5 Lyria Bennett Moses, „Agents of Change: How the Law 'Copes' with Technological Change", *Griffith Law Review* 20, 4 (2011): 763–794, https://doi.org/10.1080/10383441.2011.10854720.

6 *Ibid.,* 767.

ir pardavėjų civilinę atsakomybę bei rinkos žaidėjų konkurenciją nustatantys teisės aktai[7]. Kai kurie akademikai inovacijas, kuriomis tik patobulinami ankstesni produkto ar paslaugos atributai, vadina inkrementinėmis, o inovacijas, kurios pakeičia egzistuojančius produktus ar paslaugas, – *radikaliomis*[8]. Inkrementiniai išradimai paprastai nesukuria didelės pridėtinės vertės, o radikalios inovacijos kraštutiniais atvejais gali lemti netgi naujos technologinės paradigmos atsiradimą, kuri gali būti naudinga ne tik išradėjui, bet ir visam pasauliui[9].

Bepiločiai orlaiviai, arba *dronai*, patenka į radikalių inovacijų kategoriją. Skaičiuojama, jog 2022 m. bepiločių orlaivių rinkos vertė pasaulyje siekė beveik 31 mlrd. JAV dolerių, iki 2030 m. ji gali pasiekti beveik 56 mlrd.[10]. Paminėtina, kad bepiločiai orlaiviai kariniams tikslams buvo naudojami netgi Pirmajame pasauliniame kare[11], bet tik neseniai, patobulinus šių prietaisų technologijas, jie pradėti naudoti privačiame sektoriuje siuntiniams pristatyti[12], vaizdams fiksuoti[13], žemėlapiams sudaryti[14], statybvietėms kontroliuoti[15]. Bepiločius orlaivius policija naudoja įrodymams rinkti, įtariamųjų ar nelegalių verslų paieškoms[16], gelbėjimo tarnybos ieško nelaimingų įvykių aukų[17]. Šie maži skraidantys aparatai yra pigūs ir lengvai valdomi, tad juos dažnai įsigyja paprasti vartotojai dėl pramogos ar norėdami pašnipinėti kaimyną[18]. Bepiločių orlaivių technologijai tobulėjant ir atsirandant vis

---

7 *Ibid.,* 768.

8 Luke A. Stewart, „The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review“, *Information Technology & Innovation Foundation,* (2010): 2.

9 *Ibid.,* 2.

10 „Industry Leading Drone Market Analysis 2022-2030 | Droneii“, 2022 m. rugsėjo 20 d., https://droneii.com/drone-market-analysis-2022-2030.

11 John Sifton, „A Brief History of Drones“, *The Nation,* 2012 m. vasario 27 d., žiūrėta 2016-02-08. Plačiau žr. http://www.thenation.com/article/brief-history-drones/.

12 *Insider Intelligence,* „Why Amazon, UPS and Even Domino's Is Investing in Drone Delivery Services“, *Insider Intelligence,* žiūrėta 2022 m. gruodžio 1 d., https://www.insiderintelligence.com/insights/drone-delivery-services/.

13 Gabby Robles, „How Drones Are Used in Photography and Cinematography - 42West“, *42 West, the Adorama Learning Center* (blog), 2021 m. gruodžio 10 d., https://www.adorama.com/alc/drones-in-cinematography-photography/.

14 „Drone Mapping Applications across Industries“, *Wingtra,* žiūrėta 2022 m. gruodžio 1 d., https://wingtra.com/drone-mapping-applications/.

15 BigRentz, „6 Ways Drones in Construction Are Changing the Industry – BigRentz“, https://www.bigrentz.com, 2022 m. vasario 16 d., https://www.bigrentz.com/blog/drones-construction.

16 Gabby Robles, „How Police Departments Are Using Drones - 42West, Adorama“, *42 West, the Adorama Learning Center* (blog), 2022 m. birželio 17 d., https://www.adorama.com/alc/police-drones/.

17 Sharifah Mastura Syed Mohd Daud ir kt., „Applications of Drone in Disaster Management: A Scoping Review“, *Science & Justice* 62, 1 (2022): 30–42, https://doi.org/10.1016/j.scijus.2021.11.002.

18 Tyler Francke, „Aurora Resident Reports Disturbing Incident of Drone Apparently Spying Through Her Window“, 2019 m. kovo 27 d., https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/, https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/.

daugiau būdų, kaip juos panaudoti, į padanges turėtų kilti vis daugiau ir įvairių dydžių profesionalų bei mėgėjų valdomų bepiločių orlaivių. Viena bepiločių orlaivių naudojimo grėsmių – privatumo apsauga, šitai pripažįsta daugelis tyrėjų[19].

Bepiločių orlaivių naudojimo taisykles nustato 2019 m. ES priimti reglamentai[20]. Kiek anksčiau, 2016 m., JAV buvo publikuotos nedidelių bepiločių orlaivių naudojimo ir sertifikavimo taisyklės[21]. 2020 m. skelbti rekomendacinio pobūdžio tarptautinių organizacijų dokumentai[22]. Visos iki šiol priimtos taisyklės reglamentuoja tiktai saugų bepiločių orlaivių naudojimą, o problemų, susijusių su privatumu, neliečia. Vienas iš svarbiausių teisės aktų ES, reglamentuojančių privatumo apsaugą, yra Bendrasis duomenų apsaugos reglamentas (toliau – BDAR), tačiau nėra aišku, kiek jis gali sureguliuoti teisinius santykius tarp bepiločių orlaivių valdytojų ir visuomenės.

Neaiškus galiojančių teisės aktų taikymas bepiločių orlaivių naudojimui, privatumo apsaugą užtikrinančio reglamentavimo trūkumas, neapibrėžtas teorinis pagrindas, kaip ateityje reguliuoti privatumą bepiločių orlaivių kontekste, – tai problemos, kurios neleis užtikrinti privataus gyvenimo apsaugos arba trukdys bepiločių orlaivių technologinei pažangai. Disertacijoje, išnagrinėjus dabartinę komercinių bepiločių orlaivių ir privatumo teisinę bazę, taip pat apibendrinus mokslininkų idėjas, siekiama pateikti tokių sprendimų, kurie ateityje būtų pritaikyti teisiniam reguliavimui bei teismų praktikai ir užtikrintų šių dviejų interesų pusiausvyrą.

Darbo objektas – privatumo apsaugos priemonės, taikomos įgyvendinant komercinių bepiločių orlaivių ir privatumo teisinį reguliavimą.

Darbo tikslas – išnagrinėti dabartinį teisinių santykių, kai naudojami bepiločiai orlaiviai, privatumo apsaugos reguliavimą bei specialųjį bepiločių orlaivių reguliavimą ir pateikti jų tobulinimo pasiūlymus.

Siekiant darbo tikslo keliami tokie mokslinio darbo uždaviniai:

1. Apibrėžti bepiločių orlaivių ištakas ir sąvoką, parodyti teisės į privatumą istorines ištakas kontinentinės ir bendrosios teisės tradicijose.
2. Atskleisti teisei į privatumą kylančias grėsmes dėl bepiločių orlaivių naudojimo.

---

19 Žr. infra notes, 24–32.

20 2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų, C/2019/1821, OJ L 152, 11.6.2019: 1–40 (Reglamentas (ES) 2019/945); 2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos, C/2019/3824, OJ L 152, 11.6.2019: 45–71 (Reglamentas (ES) 2019/947).

21 Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems“, FAA– 2015–0150, Federal Register, 81, 124 (2016): 42064–42214.

22 ICAO model UAS regulations part 101 and 102, (2020); ICAO model UAS regulations part 149, (2020); ICAO Advisory Circular (AC) 101-1, (2020); ICAO Advisory Circular (AC) 102-1, (2020); ICAO Advisory Circular (AC) 102-23, (2020); JARUS UAS Operational Categorization (2019).

23 BDAR.

3. Išanalizuoti, kokias privatumo apsaugos priemones siūlo specialusis bepiločių orlaivių reguliavimas.
4. Išnagrinėti, kokias privatumo apsaugos priemones siūlo su privatumu viešoje erdvėje susijęs reguliavimas ir mokslinis diskursas.
5. Išanalizuoti privatumo apsaugos priemones, taikomas reguliuojant teisinę duomenų apsaugą.
6. Pateikti siūlymų dėl bepiločių orlaivių reguliavimo ateityje.

Mokslinio darbo naujumas ir jo reikšmė. Disertacija nauja ir reikšminga šešiais aspektais: visų pirma, mokslinėje literatūroje teigiama, jog bepiločiai orlaiviai kelia grėsmę privatumui, bet konkretūs privatumo pažeidimai detaliau nėra aptariami. Šioje disertacijoje identifikuojama, kokias grėsmes bepiločiai orlaiviai kelia privatumui, ir panaikinama esama spraga mokslinėje literatūroje. Antras aspektas yra tas, kad iki šiol nebuvo atlikta tyrimų, kuriuose būtų analizuojama, kokias privatumo apsaugos priemones suteikia specialusis bepiločių orlaivių reguliavimas. Taigi disertacijoje atliekama ES, JAV ir tarptautinių organizacijų specialiųjų bepiločių orlaivių teisės aktų analizė, kuri leistų nustatyti, ar esamos privatumo apsaugos priemonės yra pakankamos. Trečias, privatumo apsaugos ribos naudojant bepiločius orlaivius labiausiai neaiškios viešojoje erdvėje. Nors mokslinės literatūros gausu, tačiau išsamių tyrimų, aptariančių bepiločių orlaivių naudojimo viešojoje erdvėje problematiką, nėra buvę. Disertacijoje atlikta privatumo viešojoje erdvėje mokslinių šaltinių (žr. 3.2 poskyrį), teisės aktų bei teismų praktikos analizė itin reikšminga. Ketvirtas, iki šiol nenagrinėta, kokias privatumo apsaugos priemones naudojant bepiločius orlaivius numato ES duomenų apsaugos reguliavimas. Todėl disertacijoje atliekama BDAR analizė, kuri parodo, ar reikia specialiojo naujųjų technologijų, tarp jų ir bepiločių orlaivių, privatumo reguliavimo. Penktas, mokslinėje literatūroje, kuri iki šiol skelbta Lietuvoje, nebuvo tinkamai parodyta paini teisės į privatumą raida ir kaip skirtingai ji suprantama bendrosios bei kontinentinės teisės tradicijų. Dėl to Lietuvos tyrėjams gali būti sunku suprasti iš esmės skirtingą privatumo apsaugą JAV, kuri dažniausiai aptariama mokslinėje literatūroje. Tai gali lemti tiek klaidingą privatumo koncepcijos interpretaciją, tiek atotrūkį nuo kontinentinės teisės tradicijos, nes dauguma mokslinių straipsnių privatumo teisės klausimais publikuoti būtent JAV autorių. Disertacijoje aptariant teisės į privatumą raidą Prancūzijoje, Vokietijoje, JAV ir Lietuvoje, nagrinėjami privatumo suvokimo skirtumai bendrosios ir kontinentinės teisės tradicijose, bei taip siekiama prisidėti prie kokybiško mokslinio diskurso privatumo tema. Šeštas, apibrėžiant bepiločių orlaivių keliamą grėsmę privatumui ir analizuojant privatumo ribas viešojoje erdvėje remiamasi žinomų teisės srities mokslininkų teorijomis, tad darbo pabaigoje daromos išvados turi tvirtą mokslinį pagrindą. Todėl disertacijoje atliktas tyrimas yra patikimas pagrindas naujoms Lietuvos teisės aktų iniciatyvoms, teismų sprendimams bei tolesniems moksliniams tyrimams, kurie būtų skirti nagrinėti bepiločių orlaivių naudojimo ir teisės į privatų gyvenimą klausimus.

Darbo struktūra. Disertacijos struktūrą sudaro įvadas, keturi skyriai, išvados ir rekomendacijos.

Pirmame skyriuje per galimus privatumo pažeidimus analizuojama, kokią grėsmę privatumui kelia bepiločių orlaivių naudojimas. Skyrių sudaro šeši poskyriai, iš jų pirmieji keturi skirti aptarti bepiločių orlaivius sąvoką ir ištakas bei privatumo koncepciją ir jos ištakas. Toliau penktajame poskyryje analizuojami atskiri privatumo pažeidimai, kuriuos gali sukelti bepiločių orlaivių naudojimas. Šeštame poskyryje pateikiamos skyriaus išvados ir disertacijos autoriaus įžvalgos apie tai, kuo bepiločiai orlaiviai skiriasi nuo kitų privatumą galinčių pažeisti technologijų.

Antras skyrius skirtas specialiųjų bepiločių orlaivių reguliavimo šaltinių analizei. Šiame skyriuje identifikuojamos specialiuosiuose bepiločių orlaivių reguliavimo šaltiniuose randamos privatumo apsaugos priemonės ir detaliai aptariama, kokią privatumo apsaugą kiekviena iš jų galėtų suteikti. Pirmame poskyryje aptariama, kaip disertacijoje suprantama *reguliavimo* sąvoka. Antrajame aptariami specialieji bepiločių orlaivių reguliavimo dokumentai, juose pateiktos bepiločių orlaivių klasifikacijos. Trečiajame atskirai analizuojamos privatumo apsaugos priemonės, skirtos bepiločiams orlaiviams reguliuoti. Paskutiniame poskyryje daromos skyriaus išvados ir pateikiamos rekomendacijos.

Trečio skyriaus tikslas – išanalizuoti, kokias privatumo apsaugos priemones siūlo su privatumo viešojoje erdvėje problematika susijusi mokslinė literatūra, teisinis reguliavimas ir teismų praktika. Šiame skyriuje nagrinėjamos bendrosios privatumo apsaugos teorijos ir jų taikymo galimybės bepiločių orlaivių kontekste. Skyriuje trys poskyriai: pirmajame aptariama privatumo viešojoje erdvėje problematika; antrajame analizuojama mokslinė literatūra, skirta privatumui viešojoje erdvėje, ir ieškoma teorinio pagrindo, kaip privatumą viešojoje erdvėje reglamentuoti ateityje; trečiajame – EŽTT ir Lietuvos teismų praktika, susijusi su privatumu viešojoje erdvėje, ir jurisprudencijos vertinimas bepiločių orlaivių kontekste.

Ketvirtame skyriuje analizuojama, kaip bepiločių orlaivių naudojimą reglamentuoja dabartinis ES duomenų apsaugos reguliavimas. Tuo tikslu pirmame poskyryje nagrinėjama, ar BDAR taikomas ir tuomet, kai naudojami bepiločiai orlaiviai. Antrame poskyryje analizuojama, kokiu pagrindu būtų galima teisėtai rinkti duomenis bepiločiu orlaiviu. Trečiame poskyryje aptariama, ar siūlomos BDAR privatumo apsaugos priemonės pakankamos, kad būtų išvengta privatumo pažeidimų dėl bepiločių orlaivių naudojimo. Ketvirtame poskyryje pateikiamas BDAR vertinimas bepiločių orlaivių kontekste. Penktame poskyryje aptariami trūkumai, atsirandantys dėl dabartinės sutikimu paremtos privatumo apsaugos sistemos. Šeštame poskyryje siūloma, kaip ateityje būtų galima keisti privatumo reguliavimą.

Toks struktūrinis sprendimas pasirinktas sąmoningai: pirma nagrinėjamos specialiosios privatumo apsaugos priemonės, kadangi jos yra tiesiogiai taikomos bepiločių orlaivių naudojimui ir yra pagrindinė prevencinė priemonė. Tik po to analizuojami bendrieji privatumo reguliavimo modeliai, kad būtų galima įvertinti, ar egzistuojantis teisinis reguliavimas yra pakankamas ir kokiais

aspektais jį galima patobulinti remiantis teoriniais principais. Tokia struktūra leidžia aiškiau nustatyti reguliavimo trūkumus ir siūlyti pagrįstus sprendimus, kurie būtų praktiškai įgyvendinami esamoje teisinėje sistemoje.

Disertacijos pabaigoje pateikiamos išvados, rekomendacijos ir literatūros sąrašas.

Ankstesnių mokslinių tyrimų apžvalga. Disertacijos rengimo laikotarpiu mokslinių tyrimų, visapusiškai atskleidžiančių jos temą, nebuvo. Tačiau daug autorių užsienyje yra paskelbę publikacijų apie bepiločių orlaivių keliamas grėsmes privatumui, iš kurių paminėtini Paulas McBride'as (2009)[24], Ryanas Calo (2011)[25], Rachel Finn ir Dawidas Wrightas (2012)[26], Uri'is Volovelsky'is (2014)[27], Rogeris Clarke'as (2014)[28], Desas Butleris (2014)[29], Margherita Bonetto (2015)[30], Jonathanas P. Westas ir Jamesas S. Bowmanas (2016)[31], Rocci'is Luppicini'is ir Arthuras So (2016)[32]. Vis dėlto pažymėtina, kad išsami analizė, kokiais būdais bepiločiais orlaiviais gali būti pažeidžiamas privatumas, iki šiol nė viename moksliniame darbe nėra atlikta. Apie privatumo apsaugos priemones, taikomas naujuosiuose bepiločių orlaivių ES reglamentuose Nr. 2019/945 ir 2019/947, trumpą straipsnį publikavo Aurelija Pūraitė ir Neringa Šilinskė (2020)[33], kitų mokslinių tyrimų šia tema disertacijos rengimo laikotarpiu nei Lietuvoje, nei užsienyje nebuvo paskelbta. Lietuvoje apie bepiločius orlaivių keliamas grėsmes yra rašęs disertacijos autorius D. Kiršys (2016)[34],

---

24 Paul McBride, „Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations", *J. Air L. & Com.* 74 (2009): 627.

25 Ryan M. Calo, „The Drone as a Privacy Catalyst", *Stanford Law Review Online* 64 (2011): 29–33.

26 Rachel L. Finn ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 28, 2 (2012): 184–194.

27 Uri Volovelsky, „Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 30, 3 (2014): 306–20, https://doi.org/10.1016/j.clsr.2014.03.008.

28 Roger Clarke, „Understanding the drone epidemic", *Computer Law & Security Review* 30, 3 (2014): 230–246, https://doi.org/10.1016/j.clsr.2014.03.002; Roger Clarke, „The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 30, 3 (2014): 286–305, https://doi.org/10.1016/j.clsr.2014.03.005.

29 Des Butler, „The Dawn of the Age of the Drones: An Australian Privacy Law Perspective", *University of New South Wales Law Journal* 37, 2 (2014): 434–470.

30 Margherita Bonetto ir kt., „Privacy in mini-drone based video surveillance", *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG),* 4 (IEEE, 2015), 1–6.

31 Jonathan P. West ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues", *Public Administration Review* 76, 4 (2016): 649–659.

32 Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy", *Technology in Society* 46, Supplement C (2016): 109–119, https://doi.org/10.1016/j.techsoc.2016.03.003.

33 Aurelija Pūraitė ir Neringa Šilinskė, „Privacy Protection in the New Eu Regulations on the Use of Unmanned Aerial Systems", *Public Security and Public Order,* 24 (2020).

34 Deividas Kiršys, „Ar bepiločio orlaivio skrydžio vykdymas žemės sklypo oro erdvėje nepažeidžia to žemės sklypo savininko nuosavybės teisės?" (Vytautas Magnus University, 2016).

taip pat A. Pūraitė, D. Bereikienė ir N. Šilinskė (2017)[35].

Publikacijų, skelbiamų užsienyje teisės į privatumą tema, yra gausu. Teoriniu požiūriu itin aktualūs Danielio Solove'o (2002–2008)[36] tyrimai, skirti teisei į privatų gyvenimą. Taip pat paminėtini R. Finn ir kt. (2013)[37] tyrėjų darbai. Vienu iš disertacijoje analizuojamų pjūvių – pagal istorinę privatumo raidą skirtingose Atlanto pusėse, teisė į privatumą Lietuvoje dar nebuvo analizuota, tuo tarpu užsienyje šį klausimą nagrinėja nemažai autorių, tarp jų aktualiausi Jameso Q. Whitmano (2003)[38], Anupamo Chanderio, Margot'os E. Kaminski ir Williamo McGeverano (2020)[39], Paulo Schwartzo (2012)[40], Oliverio Diggelmanno ir Marios Nicole'ės Cleis (2014)[41], Raymondo Wackso (1980)[42], Richardo A. Posnerio (1981)[43], André Bertrand'o (1999)[44], Rudolfo von Jheringo (1869)[45] darbai. Apie teisę į privatų gyvenimą kituose kontekstuose, kurie galėtų būti iš dalies susiję su bepiločių orlaivių naudojimu, Lietuvoje rašė Gediminas Bučiūnas (2010, 2015)[46], Kamilė Mekšriūnaitė (2019)[47], Toma Razmaitė (2014)[48].

---

35 Aurelija Pūraitė, Daiva Bereikienė ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania", *Baltic Journal of Law & Politics* 10, 2 (2017): 107–132.

36 Daniel J. Solove, „Conceptualizing Privacy", *California Law Review* 90, 4 (2002): 1087–1156; Daniel J. Solove, „Understanding privacy", 2008; Daniel J. Solove, „I've got nothing to hide and other misunderstandings of privacy", San Diego L. Rev. 44 (2007): 745; Daniel J. Solove, „A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154, 3 (2006): 477–564; Daniel J. Solove, „Introduction: Privacy self-management and the consent dilemma", Harv. L. Rev. 126 (2012): 1880.

37 Rachel L. Finn, David Wright ir Michael Friedewald, „Seven types of privacy", *European data protection: coming of age* (Springer, 2013), 3–32.

38 James Q. Whitman, „The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal* 113, 6 (2004): 1151–1222.

39 Anupam Chander, Margot E. Kaminski ir William McGeveran, „Catalyzing Privacy Law", *Minnesota Law Review* 105, 4 (2021): 1733–1802.

40 Paul M. Schwartz, „The EU-US privacy collision: a turn to institutions and procedures", *Harv. L. Rev.* 126 (2012): 1966.

41 Oliver Diggelmann ir Maria Nicole Cleis, „How the Right to Privacy Became a Human Right", *Human Rights Law Review* 14, 3 (2014 m. rugsėjo 1 d.): 441–458, https://doi.org/10.1093/hrlr/ngu014.

42 Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).

43 Richard A. Posner, „The economics of privacy", *The American economic review* 71, 2 (1981): 405–409.

44 André Bertrand, *Droit à la vie privée et droit à l'image* (Lexis Nexis, 1999).

45 Rudolf von Jhering, *Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung,* t. 2 (Breitkopf und Härtel, 1869).

46 Gediminas Bučiūnas, „Vaizdo registratoriai ir asmens privatumas", *Mokslo taikomieji tyrimai Lietuvos kolegijose* 1, 11 (2015): 64–68; Gediminas Bučiūnas, „Sekimas ir asmens privatumas: kur riba?" (Vilnius: Mykolo Romerio universitetas, 2010).

47 Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu" (Vilnius: Mykolo Romerio universitetas, 2019).

48 Toma Razmaitė, „*Google Street View* atvejis: teisės į privatumą ir technologijų plėtros santykis" (Vilnius: Mykolo Romerio universitetas, 2014).

Mokslinių publikacijų privatumo viešojoje erdvėje aspektu, Lietuvoje nėra. Todėl atliekant šią tyrimo dalį daugiausia dėmesio skirta užsienio mokslininkų darbams, nors ir juose konkrečiai nerašoma apie bepiločių orlaivių naudojimą, – tai Helen'os Nissenbaum (1998)[49], Joelio R. Reidenbergo (2014)[50], M. E. Kaminski (2015)[51].

BDAR bepiločių orlaivių kontekste nei Lietuvos, nei užsienio tyrėjų išsamiai iki šiol neanalizuotas. Kitais aspektais, kurie gali būti susiję su bepiločių orlaivių naudojimu, BDAR buvo nagrinėtas, pvz., Aurimo Šidlausko (2019)[52], Mamoonos Asghar ir kt. (2019)[53], Jane'ės Andrew ir Maxo Bakerio (2021)[54], Yolos Georgiadou, Rolfo A. de By'aus ir Ouranios Kounadi (2019)[55], Geraldo Spindlerio ir Philippo Schmechelio (2016)[56], Piero A. Bonatti'io ir Sabrinos Kirrane (2019)[57] darbuose.

Apibendrinant galima teigti, kad nei Lietuvoje, nei užsienyje iki šiol nėra tyrimų, kurie atskleistų bepiločių orlaivių naudojimo keliamą grėsmę privatumui. Taip pat nėra mokslinių straipsnių, kurie identifikuotų ir išsamiai analizuotų, kaip specialiuosiuose bepiločių orlaivių reguliavimo šaltiniuose apibrėžtos privatumo apsaugos priemonės. Nėra ir mokslinių publikacijų, kuriose būtų analizuojama, kaip BDAR taikomas bepiločiams orlaiviams.

Mokslinio tyrimo metodologija. Rengiant šią disertaciją buvo taikyti keli mokslinio tyrimo metodai.

Dokumentų analizės metodas naudotas pirminiams informacijos šaltiniams atrinkti ir suprasti. Analizuoti duomenų šaltiniai gali būti grupuojami į keturias pagrindines kategorijas. Pirma, Lietuvos ir užsienio tyrėjų moksliniai darbai, aprašantys bepiločių orlaivių naudojimą. Antra, teoriniai moksliniai darbai, susiję su teise į privatų gyvenimą. Trečia, moksliniai darbai, teismų praktika ir

---

49 Helen Nissenbaum, „Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy* 17, 5/6 (199): 559–596.

50 Joel R. Reidenberg, „Privacy in Public", *University of Miami Law Review* 69, 1 (2014): 141–160.

51 Margot E. Kaminski, „Regulating Real-World Surveillance", *Washington Law Review* 90, 3 (2015): 1113–1166.

52 Aurimas Šidlauskas, „Video Surveillance and the GDPR", 2019.

53 Mamoona Asghar ir kt., „Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective", *IEEE Access* 7 (2019 m. rugpjūčio 9 d.): 111709–111726, https://doi.org/10.1109/ACCESS.2019.2934226.

54 Jane Andrew ir Max Baker, „The general data protection regulation in the age of surveillance capitalism", *Journal of Business Ethics* 168, 3 (2021): 565–578.

55 Yola Georgiadou, Rolf A. de By ir Ourania Kounadi, „Location Privacy in the Wake of the GDPR", *ISPRS International Journal of Geo-Information* 8, 3 (2019): 157, https://doi.org/10.3390/ijgi8030157.

56 Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): [i]-177.

57 Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR", *2019 IEEE International Congress on Big Data (BigDataCongress)* (2019 IEEE International Congress on Big Data (BigData Congress), Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.

teisės aktai, skirti privatumui viešojoje erdvėje. Ketvirta, moksliniai darbai, teisės aktai ir teismų praktika, susijusi su ES duomenų apsaugos reglamentavimu.

Renkant duomenis tyrimui naudotasi Mykolo Romerio universiteto bibliotekos ištekliais bei prenumeruojamomis duomenų bazėmis, taip pat užsienio valstybių bibliotekų fondais ir universitetų duomenų bazėmis, moksliškai patikimais elektroniniais leidiniais. EŽTT, LAT praktikos ieškota per platformas „Infolex“, „eTeismai“, „Liteko“, duomenų bazėje „HUDOC“. Lietuvos ir užsienio valstybių teisės aktų ieškota oficialiuose jų įstatymų leidžiamosios valdžios, teisės aktų skelbimo tinklalapiuose.

Istorinis metodas taikytas istorinėms prielaidoms, leidusioms susiformuoti tokiems moderniems bepiločiams orlaiviams, kokie šiais laikais naudojami, atskleisti. Šis metodas taip pat naudotas siekiant parodyti teisės į privatų gyvenimą ištakas Prancūzijoje, Vokietijoje, JAV ir Lietuvoje.

Sisteminės analizės metodas. Taikant šį metodą bendrasis privatumo ir specialusis bepiločių orlaivių reglamentavimas išnagrinėtas sistemiškai, atskleidžiant jų naudojimo ir privatumo santykį.

Palyginamoji analizė atlikta siekiant nustatyti skirtingose teisės sistemose susiformavusį privatumo suvokimą, specialiųjų bepiločius orlaivius reglamentuojančių teisės aktų nuostatas skirtingų organizacijų priimtuose dokumentuose, privatumo viešojoje erdvėje teorijas.

Analitinis kritinis metodas taikytas reaguojant į skirtingų organizacijų priimto specialiojo bepiločių orlaivių reguliavimo, EŽTT ir Lietuvos teismų praktikos, ES duomenų apsaugos teisės aktų trūkumus bei jų įgyvendinimo sunkumus, taip pat mokslinėje literatūroje siūlomų teisinio reguliavimo sprendimų trūkumus.

Ginamieji teiginiai

1. Bepiločiai orlaiviai pasižymi savybėmis, kurių neturi jokia kita iki šiol naudota privatumą galinti pažeisti technologija – ji prisideda prie ribų tarp virtualaus ir realaus pasaulio nykimo, gali būti plačiai naudojama, leidžia vykdyti intensyvią stebėseną įvairiais kampais, turi potencialą būti panaudota kaip ginklas ir yra sunkiai pastebima. Todėl ES, JAV ir tarptautinis specialusis bepiločių orlaivių reguliavimas, orientuotas labiau į saugumo užtikrinimą ir paremtas savarankiško privatumo valdymo paradigma, yra nepakankamas siekiant tinkamai apsaugoti privatumą ir sukuria poreikį specialiojo reguliavimo tobulinimui.

2. Dabartinė teisinė privatumo apsaugos sistema yra paremta savarankiško privatumo valdymo paradigma. Siekiant efektyvesnės privatumo apsaugos bepiločių orlaivių naudojimo kontekste, kuriant jų reguliavimą ateityje reikėtų vadovautis paternalistine ribų valdymo teorija.

Mokslinio tyrimo rezultatų aprobavimas ir sklaida

Dalis disertacijoje atlikto tyrimo buvo paskelbta mokslo žurnaluose „Baltic Journal of Law & Politics“, „Teisės apžvalga“ bei mokslinėje knygoje „In Future Law, Ethics, and Smart Technologies“:

Kiršienė, Julija, Christopher Kelley, Deividas Kiršys ir Juras Žymančius. „Rethinking the Implications of Transformative Economic Innovations: Mapping Challenges of Private Law“. *Baltic Journal of Law & Politics* 12, 2 (2019): 47–77.

Kiršys, Deividas, „Dronų grėsmė privatumui: galimi pažeidimai“, *Teisės apžvalga,* 1 (2021): 64–87.

Kiršienė, J., Gruodytė, E., & Kiršys, D. (2023). Transformative Smart Technologies: Mapping Challenges of Private Law. In Future Law, Ethics, and Smart Technologies (pp. 30-47). Brill.

Dalis tyrimo rezultatų taip pat pristatyta mokslo renginiuose:
2020 m. vasario 20 d. skaitytas pranešimas tema „Do drones infringe on our right to privacy?“ tarptautinėje mokslinėje konferencijoje „Future Law, Ethics, and Smart Technologies“.

2020 m. lapkričio 6 d. skaitytas pranešimas tema „Ar dronų naudojimas pažeidžia teisę į privatumą“ VDU Teisės fakulteto rengiamose dirbtuvėse „Teisinės problemos skaitmeninėje visuomenėje“.

1. BEPILOČIŲ ORLAIVIŲ KELIAMA GRĖSMĖ PRIVATUMUI

Bepiločiai orlaiviai kelia grėsmę privatumui – tai pripažįsta daugelis tyrėjų[58]. Visgi mokslininkai siekdami parodyti, kokiais būdais teisė į privatumą pažeidžiama, apsiriboja vienu ar keliais pavyzdžiais. Kitaip tariant, nors mokslinėje literatūroje pripažįstama, kad grėsmė egzistuoja, bet konkretūs privatumo pažeidimai, kylantys dėl bepiločių orlaivių naudojimo, išsamiai nenagrinėjami. Iš to atsiranda kita problema: neidentifikavus realių privatumo pažeidimų, sunku nustatyti, kokių priemonių reikėtų imtis, kad privatumas nebūtų pažeidžiamas ateityje. Šiame disertacijos skyriuje siekiama identifikuoti, kokias konkrečias grėsmes bepiločiai orlaiviai kelia privatumui. Tačiau prieš pradedant nagrinėti teisinius klausimus, susijusius su bepiločiais orlaiviais ir privatumu, vertėtų trumpai aptarti, iš kur kilo technologija, šiais laikais vadinama bepiločiais orlaiviais, apžvelgti įvairius jų terminus, pateikiamus skirtinguose šaltiniuose, taip pat suprasti iš kur kilo toks privatumo suvokimas, kokį žinome šiais laikais.

Šis skyrius, susidedantis iš šešių poskyrių, įgyvendina pirmąjį ir antrąjį disertacijos uždavinius. Pirmame poskyryje aptariama bepiločio orlaivio sąvoka, antrajame analizuojamos istorinės bei technologinės bepiločių orlaivių ištakos. Trečiame poskyryje aptariama privatumo koncepcijos problematika, ketvirtajame – istorinės privatumo ištakos. Galiausiai penktame poskyryje pereinama prie konkrečių privatumo pažeidimų, kuriuos gali sukelti komercinių bepiločių orlaivių naudojimas. Skyrius užbaigiamas šeštuoju poskyriu, kuriame apibendrinama kuo bepiločiai skiriasi nuo kitų privatumą galinčių pažeisti technologijų. Juo bus grindžiama tolesnių disertacijos skyrių analizė, kuri vertins teisinį bepiločių orlaivių ir privatumo reguliavimą.

1.1. Bepiločio orlaivio sąvoka

Sąvoka *dronas* plačiąja prasme apibūdina tiek skraidančias bepilotes transporto priemones, tiek antžemines bepilotes sistemas. Abiejų rūšių *dronai* turi vieną bendrą vardiklį: jie gali atlikti užduotis, kurios būtų sudėtingos ar netgi neįmanomos žmogui. Nepaisant plačių panaudojimo galimybių, populiaria drono sąvoka įvardyti būtent skridimo galimybes turinčias sistemas pamėgo ne tik žurnalistai, bet ir mokslininkai bei valdžios institucijų darbuotojai. Tačiau teisės aktuose dažniau vartojami alternatyvūs skraidančių dronų pavadinimai, kurie tiksliau apibūdina drono galimybę skristi. Pvz., JAV institucijos dažniausiai vartoja terminą *Unmanned Aerial Systems* (UAS), ES ir ICAO vartoja terminą *Unmanned Aircraft Systems* (UAS).

58 Žr. disertacijos įvado poskyrį „Ankstesnių mokslinių tyrimų apžvalga“.

Unmanned Aircraft System arba *Unmanned Aerial System* sąvokos plačiausiai apibūdina skraidančius dronus, kadangi į jas įtrauktas ne tik skraidantis komponentas, bet ir palaikantys komponentai, tokie kaip valdymo pultas, navigacijos įranga, kliūčių vengimo įranga ir pan. Šios sąvokos įtraukia tiek nuotoliniu būdu valdomus, tiek autonominius dronus. Nuotoliniu būdu valdomiems bepiločiams orlaiviams apibūdinti institucijos naudoja ir atskirą terminą *Remotely Piloted Aircraft Systems* (RPAS), kuris logiškai įtraukia nuotoliniu būdu valdomą skraidantį komponentą (angl. *Remotely Piloted Aircraft*) bei antžeminę valdymo stotį (angl. *Ground Control Station*)[59]. ES dokumentuose sąvoka dronas (angl. *drone*) vartojama kaip bendrinis terminas, neatsižvelgiant, ar dokumente rašoma apie visą sistemą (UAS), ar vien tik apie skrydį vykdančią dalį (UAV), bet įtraukiant nuotoliniu būdu (RPAS) ir autonominiu būdu valdomus dronus[60]. Lietuvoje skrydį vykdyti dalis vadinama *bepiločiu orlaiviu*[61].

Skirtingos jurisdikcijos dronus apibūdina skirtingai, vis dėlto turint omenyje, jog droną sudaro daug komponentų, be kurių skrydis būtų neįmanomas, ir siekiant aiškumo – visa bepiločio orlaivio sistema (UAS) disertacijoje vadinama *bepiločiu orlaiviu*.

1.2. Bepiločių orlaivių ištakos

1.2.1. Istorinės ištakos

Aviacijos istorija prasidėjo 1783 m. Tais metais karšto oro balionas, pilotuojamas Jeano François Pilâtre de Rozier ir François Laurent'o d'Arlandes'o, pakilo iš Paryžiaus centro ir skrido apie 25 min. iki jo priemiesčio[62]. Nuo to laiko žmonės pradėjo skraidyti ir skraidė su lengvesniais už orą pilotuojamais orlaiviais. Tik 1891 m. įvyko pirmasis skrydis sunkesniu nei oras sklandytuvu, o dar vėliau, 1903 m., broliams Wrightams pavyko pakilti sunkesniu už orą, varikliu varomu ir žmogaus pilotuojamu orlaiviu[63].

Vienas didžiausių išbandymų aviacijos istorijoje, su kuriuo susidūrė aviatechnikos kūrėjai, buvo orlaivių valdymas. Nuo pirmojo skrydžio lėktuvu, varomu varikliu, praėjus per 100 metų, orlaiviams, pilotuojamiems žmogaus, buvo skiriamas visas tiek verslo, tiek entuziastų dėmesys, o bepiločiai orlaiviai laikyti tiesiog išimtimi ir naujove. Nors bombardavimui bepiločiai oro balionai naudoti ir

59 Alkobi, *infra note,* 68.

60 *Ibid.*

61 „Bepiločių orlaivių reglamentai ir scenarijai", žiūrėta 2022 m. gruodžio 2 d., https://ltsa.lrv.lt/lt/veiklos-sritys/oro-transportas-1/bepilociai-orlaiviai/bepilociu-orlaiviu-reglamentai-ir-scenarijai.

62 Jonathan B. Clark, „Overview of Balloon Flights and Their Biomedical Impact on Human Spaceflight", *Handbook of Bioastronautics,* (2021), 839–856.

63 „History of Aviation – First Flights". Avjobs, Inc. Žiūrėta 2016 m. vasario 15 d. http://www.avjobs.com/history/index.asp.

XIX a. viduryje[64], visgi techniškai sudėtingesnių ir panašesnių į dabartinius bepiločius orlaivius istorija sietina su Pirmojo pasaulinio karo pradžia[65]. Tuo metu JAV kariuomenė ir laivynas eksperimentavo su oro torpedomis ir skriejančiomis bombomis. Bepiločių orlaivių gamyba itin padidėjo Antrojo pasaulinio karo metais, kai JAV kariuomenė pasirašė kontraktą su kompanija „Radioplane" ir nupirko daugiau kaip 3800 radijo ryšiu kontroliuojamų bepiločių orlaivių. Šaltojo karo metu bepiločiai orlaiviai, naudoti kariniais tikslais, stipriai keitėsi – nuo per nuotolį valdomų raketų iki sudėtingų naikintuvų[66].

Dar visai neseniai bepiločiai orlaiviai buvo brangūs, sudėtingos technologijos „paukšteliai", kuriuos galėjo įsigyti tik valstybės savo karo pajėgoms stiprinti. Vis dėlto technologinė pažanga, įvykusi robotikos srityje, padarė bepiločius orlaivius prieinamus ir visuomenei. Paprasčiausius, į delną telpančius, bepiločiu orlaivius jau galima įsigyti internetu už 20–30 eurų, o dideli ir galingi komerciniai gali kainuoti 3 000–5 000 eurų. Kai bepiločiai orlaiviai tapo prieinamesni, visuomenė savo dėmesį perkėlė nuo žmogaus valdomų orlaivių į bepiločius.

Dauguma bepiločių orlaivių, kuriuos gali įsigyti civiliai, valdomi nuotoliniu būdu, tad būtent ši grupė kelia daugiausia diskusijų. Tobulėjant technologijoms domimasi ir autonominiais bepiločiais orlaiviais, kurie programuojami iš anksto ir gali judėti be žmogaus. 2012 m. TED vykusi profesoriaus Vijay'aus Kumaro prezentacija[67] tą domėjimąsi tik paskatino, o JAV kompanijos „Amazon" 2013 m. paskelbta žinia, kad planuoja bepiločiais orlaiviais pristatinėti siuntas[68], dar labiau padidino.

Taigi bepiločiai orlaiviai yra viena pažangiausių technologijų, kurios vystymasis tęsiasi jau per 100 metų. Galima teigti, jog nepilotuojami oro balionai, vykdę bombardavimus Pirmojo pasaulinio karo metais, buvo naudoti kaip pirmieji bepiločiai orlaiviai, o vėliau tiek per Antrąjį pasaulinį karą, tiek per Šaltąjį jie buvo ne tik naudoti karo pramonėje, bet ir tobulinti – nuo oro torpedų iki radijo bangomis valdomų raketų ir sudėtingų naikintuvų. Komercinių bepiločių orlaivių istorija prasidėjo vos prieš dešimtmetį, tačiau jų technologija nėra tokia nauja. Jie

---

64 1849 m. austrai panaudojo bepiločius oro balionus, prie kurių buvo pritaisyta po vieną bombą Venecijai bombarduoti. Millbrooke, Anne, Aviation History (Englewood: Jeppesen, 2006), 1–20.

65 John F. Keane ir Stephen S. Carr, „A brief history of early unmanned aircraft". *Johns Hopkins APL Technical Digest* 32, 3 (2013): 558–571.

66 Ankstyvaisiais 1960-aisiais kompanija „Ryan Aeronautical" suprojektavo ir pagamino per 20 skirtingų savo garsiojo taikiniams naikinti skirto bepiločio orlaivio „Lightning Bug" versijų. Naudojant šį bepilotį orlaivį Vietnamo kare buvo atliktos 3435 misijos. „Lightning Bug" dizainas padarė didelę įtaką bepiločių orlaivių istorijai, iki šiol tebenaudojamas. *Ibid.,* 567.

67 „The James Bond of Robots: Vijay Kumar at TED2012 | TED Blog", žiūrėta 2022 m. gruodžio 2 d., https://blog.ted.com/the-james-bond-of-robots-vijay-kumar-at-ted2012/.

68 Jackie Alkobi, „The Evolution of Drones: From Military to Hobby & Commercial", *Percepto* (blog), 2019 m. sausio 15 d., https://percepto.co/the-evolution-of-drones-from-military-to-hobby-commercial/.

susideda iš daugybės komponentų, kurie formavosi skirtingais moderniosios visuomenės vystymosi etapais. Bepiločių orlaivių technologines ištakas vertėtų panagrinėti detaliau kitame poskyryje.

1.2.2. Technologinės ištakos

Žiniasklaidai pranešus apie naują technologiją, galima tik pasvarstyti, kokių išskirtinių gebėjimų reikia išradėjui, ją sukūrusiam. Tačiau pradėjus gilintis paaiškėja, kad tas išradimas apima jau anksčiau išrastas ir užrašytas technologijas, o naujoji tiesiog kūrybingai visa tai sujungė ir „išrado" tai, kas dar buvo nematyta. Taigi dauguma naujųjų technologijų toliau vysto ankstesnius technologinius sprendimus.

Nors ankstesnių technologijų sukeltiems teisinių santykių pokyčiams sureguliuoti įstatymų leidėjai buvo sukūrę teisinį reglamentavimą, visgi technologijoms vystantis dažnai taisykles reikia kurti iš naujo. Rinkoje pasirodžius naujosioms technologijoms kyla neapibrėžtumo jausmas, daugumą susidariusių situacijų tenka vertinti taikant pasenusias taisykles arba intuiciją. Tačiau kaip naujosios technologijos siejasi su ankstesnėmis, taip ir teisės aktai, reglamentuojantys ankstesnes technologijas, siejasi su dar ankstesnių technologijų reglamentavimu. Kitaip tariant, naujai rengiamas teisinis reglamentavimas remiasi anksčiau priimtais teisiniais sprendimais ir ieško panašumų jau esančiuose teisės aktuose. Taip pat ir bepiločių orlaivių teisinio reguliavimo pagrindų galima ieškoti nagrinėjant susijusių technologijų teisinį reguliavimą.

Pasak Adamo Rothsteino, bepiločiai orlaiviai yra panašūs į kitas keturias technologijas: į *automobilius*, nes automobilių, kaip ir bepiločių orlaivių, masinis naudojimas sukėlė transporto paradigmos poslinkį; orlaivius, nes orlaiviai, kaip ir bepiločiai orlaiviai, gali skraidyti; *kompiuterius*, nes kompiuteriai, kaip ir bepiločiai orlaiviai, turi elektroninio skaičiavimo įrenginius; bei *robotus*, nes robotai, kaip ir bepiločiai orlaiviai, tam tikrus veiksmus gali atlikti automatiškai[69].

Pasak R. Clarke'o, bepiločių orlaivių naudojimo reglamentavimo problemos neatsiejamos nuo funkcijų, kurios jiems pritaikytos iš kitų technologijų. Pvz., bepilotis orlaivis labai panašūs į *kompiuterį*, nes signalus, gautus iš valdymo pulto ir skraidomojoje dalyje įtaisytų jutiklių (tokių kaip vaizdo kameros, termometro, akcelerometro, pakreipimo ar kliūčių vengimo), analizuoja ir konvertuoja į naudojamą formą. Antra, kadangi skraidomojoje bepiločio orlaivio dalyje vidinius komponentus reikia nuolatos reguliuoti kad jie veiktų tiksliai, t. y. reikia atnaujinti programinę įrangą, keisti vidinio kompiuterio nustatymus, užtikrinti patikimą duomenų ryšį, yra būtina duomenų perdavimo ir komunikacijos funkcija, kaip ir *telekomunikacijoms*. Trečia, bepiločių orlaivių atliekami skaičiavimai ir vidiniai įrenginiai kartu su valdymo stoties įranga bei kitais duomenų šaltiniais (tokiais kaip GPS palydovai) daro juos labai panašius į *robotus*. Robotai, pirma, yra programuojami, t. y. kūrėjas, kaip panorėjęs, gali programuoti skaičiavimo arba

69 Adam Rothstein, *Drone,* Object Lessons (London: Bloomsbury Academic, 2015).

manipuliavimo simbolius, ir, antra, jiems reikia mechaninio judėjimo galimybių, t. y. ne tik funkcionuoti kaip duomenų apdorojimo įrenginys, bet ir veikti savo aplinkoje (kaip mašina). Ketvirta, nuotoliniu būdu valdomi bepiločiai orlaiviai kartu su valdytoju, pasak R. Clarke'o, gali būti vadinami *kiborgais*. Kontroliuodami nuotoliniu būdu valdomus bepiločius orlaivius pilotai pasikliauja duomenų ryšiu ir technologijomis, kurios atgamina fizinės realybės vizualizaciją (pvz., telefono ar kompiuterio ekranai; virtualios realybės technologijos; programinė įranga, gebanti atkurti erdves, supančias bepilotį orlaivį, 3D projekcijomis ir t. t.). Norėdami nuotoliniu būdu perduoti tam tikrą komandą valdytojai gali naudoti klaviatūras, mygtukus, rankenėles, kompiuterines peles, vairalazdes, gestus atpažįstančias sąsajas ar laidines pirštines. Kiborgą R. Clarke'as apibrėžia kaip žmogų, kuris turi bent vieną protezą arba ortozę. Protezas suprantamas kaip artefaktas, kuris grąžina žmogui prarastą funkcionalumą (tai gali būti ramentas, neįgaliojo vežimėlis, kontaktiniai lęšiai, klausos aparatai, pakaitinis klubas, širdies stimuliatorius ir t. t.), o ortozė yra suprantama kaip artefaktas, kuris praplečia žmogaus galimybes taip, kad jis gali atlikti tai, kas normaliam žmogui neįmanoma (tai gali būti teleskopas, mikroskopas, kosmonauto kostiumas, motorizuotas neįgaliojo vežimėlis, vaizdo projekcija į žmogaus akį, pvz., iš kameros, pritaisytos žmogaus pakaušyje, erdvinių gestų atpažinimo technologija, akies tinklainės ar lęšio implantas, kurio teikiamos galimybės pranoksta normalius žmogaus gebėjimus, ir t. t.). Bepilotis orlaivis pagal šį apibrėžimą laikytinas ortoze, kuri nuotoliniu būdu jį valdančiam pilotui suteikia gebėjimų, nebūdingų normaliam žmogui, o bepiločio orlaivio valdytojas – kiborgu[70].

Darbo problematika yra susijusi su privatumo apsauga, kuriai didžiausią grėsmę kelia asmens duomenis gebantys rinkti bepiločių orlaivių komponentai, nepakankamai apsaugota duomenų ryšio linija, nepatikima asmens duomenis apdorojanti jų programinė įranga. Pagal privatumo aspektus bepiločiai orlaiviai panašiausi į tris technologijas:

1. *vaizdo kameras,* nes šiomis, kaip ir bepiločiais orlaiviais, galima rinkti didelius kiekius asmens duomenų realiame pasaulyje;
2. *kompiuterius,* nes šie, kaip ir bepiločiai orlaiviai, naudoja programinę įrangą, kuria surinkti duomenys analizuojami ir konvertuojami į standartizuotą formatą;
3. *telekomunikacijas,* nes šiomis, kaip ir bepiločiais orlaiviais, duomenys gali būti perduodami iš vienos vietos į kitą.

Taigi vertėtų panagrinėti teisinę ir mokslinę literatūrą, susijusią su šiomis technologijomis. Teisės aktuose ir akademinėje literatūroje siūlomi sprendimai minėtoms, į bepiločius orlaivius panašioms technologijoms sureguliuoti nebūtinai bus pritaikomi, tačiau jie gali padėti rasti atramos tašką jų reglamentavimo problemoms

70 Roger Clarke, „What drones inherit from their ancestors", *Computer Law & Seurity Review* 30, 3 (2014): 247–262, https://doi.org/10.1016/j.clsr.2014.03.006.

spręsti. Pvz., teisinių šaltinių, susijusių su vaizdo stebėjimu stacionariomis vaizdo kameromis, analizė turėtų atskleisti, kokios privatumo apsaugos asmenys gali tikėtis, kad apribotų ar išvengtų stebėsenos bepiločiais orlaiviais. Literatūros, susijusios su duomenų apdorojimu, analizė, gali padėti suprasti, ar egzistuoja programiniai būdai, leidžiantys apsaugoti privatumą pačioje skraidyklėje. Telekomunikacijų reglamentavimo analizė gali padėti rasti atsakymus, kaip apsaugoti bepiločių orlaivių duomenų ryšį nuo įsilaužėlių.

1.3. Privatumo koncepcija

Visuotinai pripažįstama, jog teisė į privatumą yra fundamentali žmogaus teisė. Tai patvirtina Tarptautinių pilietinių ir politinių teisių paktas, kurį ratifikavo 167 pasaulio šalys, tarp jų ir Lietuva. Šio dokumento 17 straipsnyje skelbiama:

> *1. Niekas neturi patirti savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, jo būsto neliečiamybę, susirašinėjimo slaptumą, neteisėto kėsinimosi į jo garbę ir orumą.*
> *2. Kiekvienas asmuo turi teisę į įstatymo apsaugą nuo tokio kišimosi arba tokių pasikėsinimų.*[71]

> Europos mastu teisė į privatumą yra įtvirtinta EŽTK, kurios 8 straipsnyje rašoma:
> *1. Kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas.*
> *2. Valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.*[72]

EŽTK kaip esminiu teisę į privatų gyvenimą įtvirtinančiu dokumentu tarptautiniu mastu vadovaujasi tiek EŽTT, tiek Lietuvos teismai.

Nepaisant visuotinio pripažinimo, visgi dėl universalios privatumo koncepcijos nėra sutarta. LAT yra paskelbęs, jog „privatus gyvenimas – tai kiekvieno žmogaus teisė gyventi taip, kaip jis nori, užmegzti ir palaikyti ryšius su kitais asmenimis, būti apsaugotam nuo savavališko kišimosi į jo asmeninį gyvenimą,

---

71 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, 171, 17 straipsnis, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.174848.

72 Council of Europe, „Convention for the Protection of Human Rights and Fundamental Freedoms“, *Council of Europe Treaty Series 005* (Strasbourg: Council of Europe, 1950), 8 straipsnis..

šio gyvenimo detalių kėlimo į viešumą. Tai sritis, kuri dėl savo asmeninio, emocinio pobūdžio negali būti formalizuota, apibrėžta privalomomis vykdyti taisyklėmis. Privataus gyvenimo laisvė – tai visiems naudingas pripažinimas, kad yra egzistencijos erdvė, kuri priklauso pačiam žmogui ir į kurią įžengti kitiems gali būti draudžiama."[73] Dar privatumas gali būti suprantamas kaip „teisė būti paliktam vienam"[74], kaip asmens galimybė nuspręsti, kada, kokiu būdu ir kokios apimties informacija apie jį bendraujant gali būti pateikiama kitiems[75], kaip būsena, kai kiti neturi ar nežino informacijos apie asmenį, kurios nėra viešuose įrašuose[76], arba kaip sudėtinė samprata, apimanti informacijos apie save patį ir fizinio bei psichinio neliečiamumo kontrolę, taip pat galimybę priimti svarbius sprendimus šeimos ir gyvenimo būdo klausimais[77].

EŽTT pabrėžia, kad baigtinė asmens privataus gyvenimo sąvoka nėra suformuota[78]. Dėl bendros privatumo koncepcijos nesutaria ir tyrėjai. Pasak jų, ilgos privatumo apibrėžimo paieškos sukėlė užsitęsusius debatus, kurie dažniausiai buvo beprasmiški[79], kad apibrėžti privatumo koncepciją nei būtina, nei pageidautina[80] arba kad teisė į privatumą neturi vieno bendro vardiklio[81].

Gali būti, jog teisę į privatumą apibrėžti sunku, nes ji nuolat keičiasi. Pvz., yra tyrėjų, manančių, kad privatumo suvokimą lemia du kintamieji – socialinis, priklausantis nuo visuomenės, ir technologinis, priklausantis nuo technologinio jos išsivystymo[82].

Technologijų vystymasis teisės į privatumą raidą gali paveikti dvejopai. Viena vertus, žmonės taip norės naudotis internetu, išmaniaisiais įrenginiais, socialiniais tinklais ar bepiločiais orlaiviais, kad lengva ranka iškeis savo privatumą[83] į jų teikiamas galimybes ir nematys didelių problemų, t. y. gali būti, jog individo privatumas, siekiant naudotis technologinių naujovių, tarp jų ir bepiločių orlaivių, potencialą, galiausiai praras prasmę ir išnyks dėl ekonominio efektyvumo[84].

---

73 LAT 2001 m. balandžio 18 d. sprendimas civilinėje byloje Nr. 3K-3-461.

74 Louis Brandeis ir Samuel Warren, „The Right to Privacy", *Harvard Law Review* 4. (1890): 193–220.

75 Alan F. Westin, „Privacy and freedom", *Washington and Lee Law Review* 25, 1 (1968): 166.

76 William A. Parent, „Recent work on the concept of privacy", *American Philosophical Quarterly* 20, 4 (1983): 341–55.

77 Judith Wagner DeCew, *In pursuit of privacy: Law, ethics, and the rise of technology* (Cornell University Press, 1997).

78 Niemietz v. Germany, No. 13710/88 (ECtHR 1992 m. gruodžio 16 d.).

79 Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).

80 Nick Taylor, „State surveillance and the right to privacy", Surveillance & Society 1, 1 (2002): 66–85.

81 Solove, „Understanding privacy", *supra note,* 36.

82 Volovelsky, *supra note,* 27: 306–320.

83 „M360", „Kyberfilosofas Alexander Bard: internetas jau perėmė mūsų gyvenimo kontrolę", žiūrėta 2018 m. spalio 15 d., https://www.delfi.lt/a/78735003.

84 Richard A. Posner, „The economics of privacy", *The American economic review* 71, 2 (1981): 405–409.

Kita vertus, tikėtina, kad, atsiradus daugiau technologinių inovacijų, privatumo apsauga įgis vis didesnę reikšmę, pvz., visuomenei nuogąstaujant dėl galimo atšalimo efekto[85]. ES teisėkūros pastangos dedamos būtent šia linkme[86]. Tai gali paskatinti privatumą saugančių technologijų (angl. *privacy-enhancing technologies*) vystymą, šiuo metu prieinamos tokios technologijos, kurios leidžia duomenis anonimizuoti, šifruoti[87], atlikti geografinį atribojimą (angl. *geofencing*)[88].

Socialinį kintamąjį taip pat sudaro du aspektai. Pirmasis susijęs su politine visuomenės santvarka, t. y. ar tai demokratinė šalis, kuriai būdinga laisva rinka, žodžio laisvė, santykinai mažas valstybės kišimasis į individų privačius reikalus, ar, atvirkščiai, komunistinė šalis, kur iš dalies ar visiškai valstybės politika reguliuoja rinką, cenzūruoja spaudą ir vykdo didelio masto piliečių stebėseną. Tikėtina, jog privatumo suvokimas liberaliose visuomenėse gyvenančių žmonių reikšmingai skirtųsi nuo tų, kurie gyvena kolektyvinėse socialistinėse šalyse. Pvz., Lietuvoje 1940–1990 m., kai galiojo socialistinė santvarka, asmuo jokio privatumo valstybėje apskritai negalėjo tikėtis.

Antras aspektas – tai teisinė šalies tradicija ir jos įtaka socialinėms normoms. Konkrečiau, kaip visuomenė suvokia, kas sudaro privataus gyvenimo turinį. Šitai lemia tiek šalies istorija, tiek šalies teisės raida. Nors dauguma Europos šalių ir JAV grindžiamos liberalia demokratija, bet žmonės, gyvenantys skirtingose šalyse, privatumą suvokia skirtingai. Pvz., kai kuriose žemyninės Europos valstybėse nudistai viešuose miesto parkuose gali būti įprastas vaizdas, o JAV tai būtų tabu. Žemyninės Europos šalyse gyvenantys žmonės sunkiai supranta JAV įžymybių vaikymosi ir paparacių kultūrą[89].

Tokiems suvokimo skirtumams suprasti reikia istorinės teisės į privatų gyvenimą raidos žinių. Kadangi disertacijoje remiamasi JAV ir Europos teisės dokumentais, prieš pradedant nagrinėti bepiločių orlaivių ir jiems taikomą privatumo reguliavimą, vertėtų paanalizuoti, kokiomis aplinkybėmis buvo sukurta koncepcija, kuri, nors abiejose Atlanto pusėse vadinama „privatumu“, bet suvokiama skirtingai.

---

85 Žr. disertacijos 1.5.1 poskyrį, taip pat Jonathon W. Penney, „Understanding Chilling Effects“, *Minnesota Law Review* 106, 3 (2022).

86 Tai plačios apimties ES legislatyvinės iniciatyvos, pvz., 2018 m. įsigaliojęs BDAR ir 2017 m. Europos Komisijos pasiūlymas dėl E. privatumo reglamento. BDAR; „Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)“ (2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A52017PC0010.

87 Johannes Heurix ir kt., „A Taxonomy for Privacy Enhancing Technologies“, *Computers & Security* 53, (2015): 1–17, https://doi.org/10.1016/j.cose.2015.05.002.

88 Tamraparni Dasu, Yaron Kanza ir Divesh Srivastava, „Geofences in the sky: herding drones with blockchains and 5G“, *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems,* 2018, 73–76.

89 Žr. daugiau Whitman, *supra note,* 38: 1153–1158.

1.4. Privatumo istorinės ištakos

Disertacija rašoma lietuvių kalba ir yra orientuota į Lietuvos bei Europos teisinę aplinką, todėl joje labiau vadovaujamasi kontinentinės teisės tradicijos privatumo suvokimu. Tačiau verta pastebėti, jog nemaža dalis mokslinių šaltinių, kuriais vadovaujamasi tyrime, yra publikuoti JAV autorių, kurie remiasi JAV privatumo suvokimu. Dėl šios priežasties ypatingai svarbu suvokti privatumo suvokimo skirtumus kontinentinės ir bendrosios teisės tradicijos šalyse, siekiant išvengti klaidingos interpretacijos ir atotrūkio nuo kontinentinės teisės tradicijos suvokimo, ypač nagrinėjant tokius klausimus kaip bepiločių orlaivių naudojimas ir jų reguliavimas. Tolesniuose poskyriuose atliekama privatumo ištakų Prancūzijoje, Vokietijoje, JAV ir Lietuvoje analizė padės geriau suprasti šiuos skirtumus ir teisingai juos interpretuoti tyrime naudojamuose moksliniuose šaltiniuose bepiločių orlaivių ir privatumo tematika.

1.4.1. Privatumo ištakos Prancūzijoje

Pirmosios „privataus gyvenimo“ apsaugos idėjos sietinos su Prancūzijos revoliucija. Tai virsmo laikotarpis, kai iš feodalinės luominės santvarkos, revoliucionierių vadinamos *ancien régime*[90], pereita į liberalią valstybę. 1791 m. rugsėjo 3 d. priimta Prancūzijos konstitucija, kuri viena pirmųjų Europoje įtvirtino konstitucinę monarchiją, joje kartu su spaudos laisve buvo garantuojama ir privatumo apsauga[91]. Pasak vieno šios konstitucijos kūrėjų, senojoje santvarkoje netgi už mažiausią turtingųjų garbės įžeidimą buvo baudžiama kaip už sunkų nusikaltimą, o prieš paprastą pilietį analogiškai nusižengus praktiškai jokių teisinių priemonių nebuvo, tad „naujoji doktrina“ yra dar labiau teisinga ir atitinka naujosios santvarkos principus[92]. Privatumo apsaugos idėja Prancūzijos konstitucijoje kilo iš visuomenės siekio turėti panašaus lygio viešąją reputaciją, kokią turėjo turtingieji, t. y. privatumas buvo suvokiamas kaip garbės apsauga.

Ir po Prancūzijos revoliucijos šios idėjos išliko, tik spauda tebebuvo cenzūruojama, todėl „nederami“ straipsniai nepasiekdavo visuomenės. Vis dėlto 1819 m., kai cenzūra buvo panaikinta[93], kartu su spaudos laisve atsirado rūpinimasis garbe ir privatumu. Pierre-Paul Royer-Collard, žymus politikas, Sorbonos universiteto filosofijos profesorius ir prancūzų liberalizmo apologetas, savo žymioje 1861-ųjų kalboje gindamas spaudos laisvę perspėjo, kad privatus gyvenimas turi būti

90 Jérôme Pétion, “Suite du discourse sur la liberté de la Presse”, 16 Courier de Provence 199 (1791).

91 Prancūzijos 1791 m. rugsėjo 3 d. Konstitucija, III skyriaus V antraštės 17 straipsnis („Les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privee, seront punies sur leur poursuite“).

92 Pétion, *supra note,* 93.

93 Christine Haynes, *Lost Illusions: The Politics of Publishing in Nineteenth-Century France* (Harvard University Press, 2010).

„atitvertas siena“ (pranc. *murée*) nuo garbės „įžeidimo“ (pranc. *calomnie*) pavojaus[94]. Nors tuo laikotarpiu dar nebuvo jokių teisės aktų, išskyrus Prancūzijos konstituciją, ar teismų praktikos, kurie detaliau atskleistų teisės į privatumą turinį, tačiau garbingas statusas ir privatus gyvenimas žmonėms buvo tokie svarbūs, kad iki pat XIX a. vidurio pagrindinis būdas šias teises apginti buvo dvikova[95].

Po kelis dešimtmečius trukusios privatumo apsaugos ginklais, ši teisė galiausiai radosi Prancūzijos teismų praktikoje. Pirmieji sprendimai, susiję su „teise į atvaizdą“, buvo priimti dar XIX a. šešto dešimtmečio pabaigoje[96]. Vieną garsiausių bylų 1867 m. iškėlė rašytojas Alexandre'as Dumas tėvas (pranc. *père*), kai viešai buvo publikuotos skandalingos jo ir meilužės nuotraukos. Rašytojas fotografui nuotraukas pardavė tiesiogiai nedrausdamas jų publikuoti, todėl teismui nagrinėjant bylą nekilo abejonių, jog nuotraukos priklausė fotografui. Tačiau pagrindinis klausimas buvo, ar net ir neturėdamas nuosavybės teisės į fotografijas A. Dumas galėjo tikėtis kokios nors apsaugos. Teismas pasisakė, jog net jeigu asmuo ir buvo išreiškęs sutikimą publikuoti gėdingas nuotraukas, jis išlaiko teisę atšauti savo sutikimą. Teismas pripažino, kad tokių nuotraukų paskelbimas gali priminti asmeniui, jog jis pamiršo pasirūpinti savo orumu, taip pat jam priminti, jog privatus gyvenimas turėtų būti saugomas dėl visuomenės ir geros moralės interesų. Teismas galiausiai įpareigojo fotografą parduoti nuotraukas A. Dumas, taip įtvirtindamas privatumo viršenybę prieš teisę į nuosavybę[97]. Iš esmės teismas pripažino, jog asmuo net ir perleidęs nuosavybės teisę į nuotraukas, savo privatumo neprarado. Taigi jau tuo metu privatumas buvo suprantamas kaip neturtinė teisė, kurios tiesiog negalima galutinai parduoti. Panašios motyvacijos Prancūzijos teismai laikėsi ir vėliau[98].

Teismų praktikoje vyravusias idėjas 1888 m. savo knygoje „Les principles du droit“ apibendrino žymus tų laikų teisės filosofas Émile'is Beaussire'as. Jis teigė, jog teisė į privatumą, kaip garbės teisių dalis, turėtų būti ginama ne per dvikovas, kaip tuo metu buvo įprasta, bet teisiniais instrumentais[99]. Panašaus požiūrio į privatumą kaip teisės į garbę dalį laikėsi ir kiti to meto prancūzų teisės teoretikai[100].

---

94 Prosper Brugière baron de (1782–1866) Auteur du texte Barante, *La Vie Politique de M. Royer-Collard: Ses Discours et Ses Écrits / Par M. de Barante,* 1861, https://gallica.bnf.fr/ark:/12148/bpt6k116929z.

95 Bertrand, *supra note,* 44: 2.

96 Sergent c. Defonds, Trib. civ. Seine, Nov. 11, 1859, 6 Annales de la Propriete Industrielle Artistique et Litteraire [A.P.I.A.L.] 168 (1860); Felix c. O'Connell, Trib. civ. S[e]ine, June 16, 1858, 4 A.P.I.A.L. 250 (1858); Soeur Melanie c. Foug6re, Ord. de R66r6, Apr. 11, 1855, 6 A.P.I.A.L. 167 (1860).

97 Dumas c. Liébert, CA Paris, 1867 m. gegužės 25 d., 13 A.P.I.A.L. (1867).

98 Moitessier c. Féral, Tribunal civil de la Seine, 1877 m. gruodžio 5 d., 23 A.P.I.A.L. (1878); Eden c. Whistler, Cass. civ., Mar. 14, 1900, D.P. (1900); Le Figaro c. Chaperon, CA Paris, 4e ch., Dec. 2, 1897, 45 A.P.I.A.L. 61 (1899).

99 Emile Beaussire, *Les principes du droit* (Alcan, 1888).

100 Alphonse Barthélemy Martin Boistel, *Cours de philosophie du droit: professé à la Faculté de droit de Paris,* t. 1 (A. Fontemoing, 1899).

Taigi teisė į privatumą kilo iš Prancūzijos revoliucijos laikų visuomenės siekio turėti tokią pačią reputacijos apsaugą, kokia buvo taikoma aukštuomenei. Garbė ir privatumas, kaip jos dalis, XIX a. prancūzams buvo tiek svarbūs, kad ši teisė buvo ginama dvikovose, o nuo XIX a. antros pusės buvo įtvirtinta teisės šaltiniuose ir ginčai dėl jų buvo pradėti spręsti teismuose. Teismai privatumą dažniausiai interpretuodavo kaip teisę į atvaizdą, kuris laikytas asmens neturtine teise ir kurios visiškai išsižadėti asmuo negali.

1.4.2. Privatumo ištakos Vokietijoje

Vokiečių teisės teoretikai XIX a. pabaigoje, kaip ir jų pirmtakai Prancūzijoje, teisę į privatų gyvenimą suvokė per teisę į garbę[101]. Tačiau, užuot rėmęsi prancūzų teisės teoretikais[102], vokiečių mokslininkai užsimojo ieškoti tvirtesnio teisinio pagrindo romėnų teisėje įtvirtintoje *inuria*[103]. Interpretuodami šią teisę per hėgelistinį suvokimą, jie iš esmės sukūrė atskirą, būtent iš Vokietijos teisės tradicijos kilusį darinį – „asmenybės" teisę (vok. *Persönlichkeitsrecht*), šiuolaikinėje Lietuvos teisėje vadinamą asmeninėmis neturtinėmis teisėmis[104].

---

101 James Q. Whitman, „Enforcing Civility and Respect: Three Societies", *Yale Law Journal* 109, 6 (2000): 1279–1398.

102 Pasak J. Whitmano, prancūzų autoriai savo idėjas grindė atmestinai parengtais to laikmečio įstatymais ir neaiškiomis socialinėmis normomis. Žr. Whitman, *supra note,* 38: 1183.

103 Iniuria turinį romėnų teisėje apibendrino Laurynas Pakštaitis: „*Iniuria (injuria)* – „neteisėtumas", nuoskauda, arba įžeidimas – dažnai pasitaikiusi ir itin plačiai traktuota veika (Giltaj, 2018, p. 23). Šią sąvoką apėmė įžeidimas, kuris turėjo būti dažniausia „neteisėtumo" atmaina pagal *Lex Cornelia de iniuriis.* Pasak tyrinėtojų, prie iniuria kaip įžeidimo atmainos galėjo būti priskirti ir fiziniai sužalojimai arba kitam asmeniui priklausančio vergo išplakimas (kaip savininko įžeidimas), arba bet koks veiksmas, užtraukiantis pažeminimą, o įžeidimo būdas taip pat turėjo teisinės reikšmės. Teigiama, kad kaip *iniuria* (nuoskauda) buvo ir sąnario sulaužymas (*membrum ruptum*), kaulo sulaužymas (*os fractum*) ir „paprastos nuoskaudos, kurias mūsų nuomone sudarė lengvi smurtai, smūgiai į veidą ir šiaip smūgiai"(Girarrd, 1932, p. 22). Dėl šių veikų galėjo būti paduodamas skundas. Teigiama, kad vėliau *Lex Cornelia de injuris* diktatorius Kornelijus Sula nuo kitų nuoskaudų atskyrė smūgius ir įsiveržimus į būstą (*puksare, verberarre, vi domum introire*), tikslu iš jų padaryti viešuosius nusikaltimus (Girard, 1932, p. 24). *Iniuria* buvo laikomas ir gyvo ar negyvo žmogaus įžeidimas, reputacijos menkinimas, dėl tokios veikos buvo galimas skundas privatinės teisės tvarka (*actio injuriarum*) (de Villiers, 1900, p. 251). Ulpianas apibrėžė *iniuria* kaip „bet ką, kas daroma ne pagal teisę" [...]. Iniuria buvo reikalaujamas noras padaryti įžeidimą – šmeižimo ir kitais iniuria veikos atvejais reikėjo nustatyti norą šmeižti elgtis neteisėtai – *animus iniuriandi.*" (žr. Laurynas Pakštaitis, „Senovės romėnų baudžiamosios teisės bruožai", Research Journal *Public security and public order* 30 (2022): 103).

104 LR civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Civilinis kodeksas, VIII-1864, *Valstybės žinios,* 2000-09-06, Nr. 74-2262, 1.114 straipsnis, „Asmeninės neturtinės teisės ir vertybės".

Pasak hėgelistų, primityvios bausmių formos, tokios kaip „akis už akį, dantis už dantį“, palaipsniui rutuliojasi į sudėtingesnes, proporcingumu paremtas bausmių koncepcijas, kurios gali plačiau aprėpti nematerialias vertybes[105]. Garsus vokiečių teisės teoretikas, R. von Jheringas, asmenybės teisę iš romėnų iniuria išvedė vadovaudamasis panašia logika, t. y. romėnų *iniuria*, kurios dvasia buvo labiau materiali, vystėsi į labiau nematerialią asmenybės teisės dvasią[106]. Jo nuomone, garbė visuomet buvo įžeidimo teisės dalis, net ir ankstyvaisiais laikotarpiais. Iš pradžių romėnai manė, jog įstatymais galima apginti tik materialųjį turtą. Tačiau garbę suprantant vis giliau, ši ankstyvoji teisinė apsauga pamažu plėtėsi, kol įstatymai apėmė visus garbės aspektus, aprėpdami ir žodinius įžeidimus, ir kitokias nepagarbos formas[107]. Taigi garbės teisės kaitą, kaip ir bausmių teisės suvokimo pokyčius, lėmė „laiko dvasios“ raida, t. y. kai primityvi vien tik piniginių interesų apsauga pamažu virto sudėtinga „neekonominių“ interesų apsauga[108]. Ta lėta raida nuo materialaus iki nematerialaus tęsiasi ir šiuolaikiniame pasaulyje, t. y. šiuolaikinės priemonės suteikia apsaugą tokioms nematerialioms vertybėms kaip atvaizdas, vardas, susirašinėjimai, prieiga prie šiuolaikinių patogumų, pvz., telegrafo ir tramvajaus[109]. Vokiečių asmenybės teisė buvo siejama ir su autoriaus teise kontroliuoti savo darbus bei reputaciją (vok. *Urheberrecht*). Šiuolaikinėje kontinentinėje tradicijoje šios teisės priskiriamos *le droit moral* arba *moral rights*[110] doktrinai, kurios atitikmuo Lietuvoje yra asmeninės neturtinės autorių teisės[111]. Tokio požiūrio nuo XIX a. pabaigos iki XX a. pradžios laikėsi ir kiti garsūs vokiečių teisės mokslininkai, pvz., Karlas Gareisas ir Josefas Kohleris[112].

Doktrinoje suformuotas dualistinis asmenybės teisės turinys persikėlė ir į teismų praktiką[113], ir teisės aktus. 1900 m. įsigaliojusiame Vokietijos civiliniame

---

105 James Q. Whitman, „Origins of Law and the State: Supervision of Violence, Mutilation of Bodies, or Setting of Prices, At the“, *Chi.-Kent L. Rev.* 71 (1995): 41.

106 Von Jhering, *supra note,* 45: 235.

107 *Ibid.,* 235.

108 *Ibid.,* 236.

109 *Ibid.,* 344–345.

110 Jill R. Applebaum, „The Visual Artists Rights Act of 1990: An Analysis Based on the French Droit Moral Notes and Comments“, *American University Journal of International Law and Policy* 8, 1 (1993): 183–224.

111 LR autorių teisių ir gretutinių teisių įstatymas, VIII-1185, *Valstybės žinios,* 1999-06-09, Nr. 50-1598, 14 straipsnis „Autorių asmeninės neturtinės teisės“.

112 Gerd Kleinheyer, „Dieter Leuze, Die Entwicklung des Persönlichkeitsrechts im 19. Jh. Zugleich ein Beitrag zum Verhältnis allgem. Persönlichkeitsrecht–Rechtsfähigkeit“, *Zeitschrift der Savigny-Stiftung für Rechtsgeschichte: Germanistische Abteilung* 81, 1 (1964): 478–80; Josef Kohler, *Das Autorrecht, eine zivilistische Abhandlung: zugleich ein Beitrag zur Lehre vom Eigenthum, vom Miteigenthum, vom Rechtsgeschäft und vom Individualrecht, t.* 6 (G. Fischer, 1880).

113 Viena garsiausių bylų kilo, kai buvo publikuotos Vokietijos imperijos kanclerio Otto von Bismarcko nuotraukos mirties patale. Tačiau Vokietijos teismai nagrinėjo ir daug kitų bylų, susijusių su asmenybės teisėmis. Žr. Whitman, *supra note* 38: 1185–1186.

kodekse buvo įtvirtintos nuostatos, suteikiančios apsaugą tokioms neturtinėms teisėms kaip vardas[114], gyvybė, kūnas, sveikata, laisvė[115] ar kredito istorija[116], o Vokietijos baudžiamasis kodeksas numatė atsakomybę už įžeidimą[117]. Šios teises saugančios nuostatos Vokietijoje galioja iki šiol. Vokietijos konstitucijos, įsigaliojusios 1949 m., 2 straipsnis ir šiandien numato, jog „kiekvienas asmuo turi teisę laisvai vystyti savo asmenybę“[118].

Taigi Vokietijoje, kaip ir Prancūzijoje, teisė į privatų gyvenimą suprantama per garbę, tačiau vokiečiai šios teisės ištakų doktrinoje pasirinko ieškoti romėnų teisėje, tokiu būdu sukurdami atskirą „asmenybės“ teisę. Ši apima neekonominių asmens interesų, tokių kaip vardas, atvaizdas, susirašinėjimai, apsaugą, taip pat autorių teisę kontroliuoti savo darbus ir reputaciją, kurie, kaip ir Prancūzijos tradicijoje, yra neatsiejami nuo asmens ir negali būti galutinai perleidžiami kitiems individams.

1.4.3. Privatumo ištakos JAV

Privatumo apsauga JAV yra kilusi iš 1789 m. paskelbtos JAV konstitucijos ketvirtosios pataisos, kuri užtikrina asmens namų, susirašinėjimo ir veiksmų apsaugą nuo nepagrįstų kratų bei areštų[119]. Vis dėlto naratyvas, jog ši nuostata asmenis apsaugo ne tik nuo fizinio įsiveržimo į asmens namų erdve, bet ir nuo nepagrįsto valstybės kišimosi į privatų gyvenimą iškilo tiktai 1886 m. *Boyd v. United States* byloje. Joje ginčas iškilo po to, kai valdžios institucijos konfiskavo į JAV uostą įvežtas prekes, nes įtarė, jog prekeivis už jas nesumokėjo muito. Tam, kad surinktų įrodymus prieš prekeivį, valdžios institucijos jo paprašė pateikti ginčijamų prekių sąskaitą. Prekeivis pateikė skundą paprašydamas teismo sąskaitos nepriimti kaip įrodymo ir ginčijo valdžios institucijų reikalavimą. Teismas pripažino, jog ginčijamų prekių sąskaita yra „privatūs dokumentai“, kurių konfiskavimas lėmė nepagrįstą valdžios institucijų įsiveržimą į asmens „namų erdvės šventumą“

114 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 6 des Gesetzes vom 7. November 2022 (BGBl. I S. 1982) geändert worden ist, § 12 Namensrecht.

115 BGB, § 823 Schadensersatzpflicht.

116 BGB, § 824 Kreditgefährdung.

117 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 11. Juli 2022 (BGBl. I S. 1082) geändert worden ist, § 185 Beleidigung.

118 Konstitucijos tekstas nepasikeitęs iki šios dienos. Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022 (*Federal Law Gazette* I p. 968).

119 JAV konstitucijos ketvirtoji pataisa („The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“)

(angl. *sanctity of the home*) ir gyvenimo privatumą (angl. *privacies of life*)[120].

1890 m., praėjus vos ketveriems metams po *Boyd v. United States* ir dvejiems metams po prancūzų teisinės patirties aprašymo moksliniame diskurse[121], JAV garsųjį straipsnį „Right to Privacy" paskelbė Samuelis Warrenas ir Louisas Brandeisas[122]. Nuo jo, manoma, ir prasidėjo privatumo teisės raida JAV[123]. Straipsnį autoriai išleido kaip atsaką į tuščias, jų nuomone, ir padorumo ribas peržengiančias paskalas spaudoje. Jų teigimu, vienintelis būdas apsaugoti asmenis nuo įkyrios spaudos ir fotografų yra „teisės į privatumą" įtvirtinimas, ši teisė teiktų apsaugą ne tik aukšto statuso individams, bet ir visai visuomenei[124]. Savo moksliniame darbe siūlomą teisę į privatumą autoriai kildina iš Prancūzijos[125] ir Vokietijos[126] teisės tradicijų, kuriose, kaip jau aptarta anksčiau, apie ją diskutuota nuo pat XVIII a. pabaigos[127].

S. Warrenas ir L. Brandeisas pripažįsta, jog bendrosios teisės tradicijoje, skirtingai nuo romėnų teisės, neegzistuoja koncepcija, pagal kurią būtų atlyginama įžeidimo ar garbės sumenkinimo padaryta žala individo psichinei sveikatai[128]. Panašus JAV teisėje nebent šmeižto (angl. *defamation*) institutas, tačiau jo esmė yra žala asmens reputacijai, o ne dvasinei sveikatai. Kitaip tariant, JAV šmeižto institutas leidžia išieškoti žalą dėl objektyvaus individo įvaizdžio sumenkinimo visuomenės akivaizdoje, bet nesuteikia galimybės kompensuoti žalos už subjektyvias asmens patirtas dvasines kančias. Vis dėlto, pasak autorių, privatumo apsaugą galima išvesti iš bendrojoje teisės tradicijoje pripažįstamų intelektinės ir autorių nuosavybės institutų. Kaip pastebima moksliniame diskurse, tai iš esmės ta pati motyvacija, kuria vadovavosi vokiečių teisės teoretikai, savo „asmenybės" teisę kūrę būtent per autoriaus teisę kontroliuoti savo darbus bei reputaciją (vok. *Urheberrecht*)[129].

Tačiau iš kontinentinės teisės tradicijos pasiskolinta privatumo teisė JAV nebuvo priimta svetingai. Tendenciją suteikti sąlyginai menką privatumo apsaugą galima pastebėti JAV teismų praktikoje, kurioje privatumo teisė balansuojama su saviraiškos laisve (angl. *freedom of expression*), kylančia iš JAV konstitucijos pirmosios pataisos[130]. Pvz., tais atvejais, kai išprievartavimo aukų vardai buvo

120 Boyd v. United States, 116 U.S. 616 (1886).
121 Emile Beaussire, *Les principes du droit* (Alcan, 1888).
122 Brandeis ir Warren, *supra note,* 77: 193.
123 Whitman, *supra note,* 38: 1151–1222.
124 Brandeis ir Warren, *supra note,* 77: 196, 214–215.
125 *Ibid.,* 214, 216, 218.
126 *Ibid.,* 198.
127 Žr. disertacijos 1.4.1. ir 1.4.2. poskyrius.
128 Brandeis ir Warren, *supra note,* 77: 198.
129 Whitman, *supra note,* 38: 1207.
130 JAV konstitucijos pirmoji pataisa („Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.")

viešai paskelbti televizijos laidoje[131] arba kai iš gerai žinomo dvasininko buvo išsityčiota laikraštyje paskelbtoje alkoholinio gėrimo reklamoje[132], teismo vertinimu, akivaizdžiai didesnį svorį turėjo saviraiškos laisvė. Nors tikėtina, jog panašiais atvejais kontinentinės teisės tradicijos šalyse, kur ypač pabrėžiama asmens garbė ir orumas, tokių bylų baigtys būtų kitokios.

JAV taip pat saugomas asmens atvaizdas. Vis dėlto amerikiečių suvokimas fundamentaliai skiriasi nuo europiečių. Maždaug XX a. viduryje JAV mokslinėje doktrinoje radosi „viešumo teisė" (angl. *right of publicity*). Joje atvaizdas neturi nieko bendra su garbe ar orumu. Tai turtinė teisė, kurią asmuo gali kada panorėjęs parduoti ir išsižadėti bet kokių pretenzijų į perleisto atvaizdo panaudojimą ateityje[133]. Tuo tarpu, kaip jau minėta ansktesniame disertacijos poskyryje, kontinentinėje teisės tradicijoje atvaizdo, kaip asmeninės neturtinės teisės, pardavimo sandoriai gali būti nuginčyti[134].

Bylose, susijusiose su JAV konstitucijos ketvirtąja pataisa, taip pat nėra teikiama pernelyg didelė reikšmė kontinentine teisės tradicija paremtam, S. Warreno ir L. Brandeiso siūlomam privatumo suvokimui. Pvz., byloje „Schmerber v. California" teismas teigė, kad Ketvirtoji pataisa suteikia apsaugą „privatumui ir orumui nuo nepagrįsto valstybės kišimosi", tačiau joje didžiausia motyvacijos dalis buvo skirta samprotavimams, susijusiems su valstybe, tuo tarpu „orumo" intereso aiškinimui daug dėmesio neskirta[135]. Taip pat „Lawrence v. Texas" sprendimo tekste kalbama apie „pagarbą" homoseksualių pažiūrų asmenims, tačiau apie „pagarbos" turinį JAV Aukščiausiasis Teismas taip pat pernelyg neišsiplečia[136]. Teisės doktrinoje pastebima esant tikimybei, jog europietiškas privatumo suvokimas, kurį bandė pristatyti S. Warrenas ir L. Brandeisas JAV teisėje per laiką išblės[137].

Taigi, JAV teisė į privatumą istoriškai kyla iš konstitucijos ketvirtosios pataisos, kuri pirmiausia saugo nuo nepagrįsto valdžios institucijų įsiveržimo į asmeninį būstą. XIX a. ši nuostata JAV teismų buvo išplėsta siekiant aprėpti ir kišimąsi į privatų gyvenimą. Nuo to laiko buvo bandymų į JAV teisę perkelti tokią pačią teisę į privatumą, kaip yra kontinentinėje teisės tradicijoje, tačiau nesėkmingai. Dėl to JAV iki šiol privatumas iš esmės suprantamas kaip laisvė nuo valstybės nepagrįsto įsikišimo į privačius individo reikalus.

131 „Cox Broadcasting Corp. v. Cohn", 420 U.S. 469 (1975).
132 „Hustler Magazine, Inc. v. Falwell", 485 U.S. 46 (1988).
133 Melville B. Nimmer, „The right of publicity", *Law and Contemporary problems* 19, 2 (1954): 203–23.
134 Žr. disertacijos 1.4.1 poskyrį; Dumas c. Liébert, *supra note,* 100.
135 „Schmerber v. California", 384 U.S. 757 (1966).
136 „Lawrence v. Texas", 539 U.S. 558 (2003).
137 Whitman, *supra note,* 38: 1151.

1.4.4. Šiuolaikinis privatumo suvokimas skirtingose Atlanto pusėse

Kaip atskleidė padaryta analizė, privatumo suvokimas kontinentinėje ir bendrosios teisės tradicijose reikšmingai skiriasi. Europoje jis suvokiamas kaip garbės ir orumo sudedamoji dalis, kuriam didžiausią grėsmę kelia žiniasklaida. JAV privatumas suvokiamas kaip laisvė nuo nepagrįsto kišimosi į individų asmeninius reikalus, kuriai didžiausią grėsmę kelia valstybė. Europoje privatumas gali būti ginamas per daugelį atskirų teisinių institutų, tokių kaip teisė į vardą, teisė į atvaizdą, teisė į garbę ir orumą, teisė į asmenybę, teisė į privatumą, teisė į būsto neliečiamybę. JAV privatumas ginamas gerokai siauriau – iš esmės tik per laisvę nuo valstybės kišimosi į individo asmeninius reikalus. Taip pat privatumo suvokimas, kaip neturtinės vertybės, yra išskirtinis kontinentinės teisės tradicijų šalių darinys, tuo tarpu JAV ši teisė suvokiama tik per turtinių santykių perspektyvą.

Skirtingos teisės į privatumą ištakos lemia ir tam tikrus teisinės kultūros skirtumus šiais laikais. Vienas tokių – skirtingai suvokiama, kaip gali būti naudojamas asmens atvaizdas. Pvz., nors Europoje asmuo gali parduoti savo nuotraukas tretiesiems asmenims ir suteikti leidimą jas publikuoti[138], bet tai nereikštų, jog tokiu sandoriu pirkėjas gautų teisę nuotraukas naudoti be jokių apribojimų, t. y. parduotas atvaizdas vis tiek negalėtų būti panaudojamas tokiu būdu, kuris pažemintų asmens garbę ar orumą[139]. Tuo tarpu JAV nuotrauka su asmens atvaizdu tėra dar viena prekė, kurią pirkėjas gali panaudoti ir tokiu būdu, kuris žemintų nuotraukoje atvaizduotą asmenį[140].

Europoje teismai į internete paskelbtas žeminančias nuotraukas žiūri labai rimtai ir beveik visada linksta į asmens, kurio nuotraukos buvo publikuotos, pusę, neteisėtai kito asmens nuotraukas paskelbusius asmenis bausdami ne tik baudomis, bet ir laisvės atėmimu[141]. Tuo tarpu JAV teismai iškilus ginčams dėl žeminančių

---

138 Pvz., Lietuvoje teisė į atvaizdą, nors ir yra asmeninė neturtinė teisė, tačiau gali turėti ir tam tikrą ekonominę vertę, nes gali būti įvertinta pinigais, taigi šiuo aspektu yra kartu ir turtinė teisė. LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.

139 LAT yra pasisakęs, kad net ir parduotos asmens nuotraukos negalima demonstruoti, atgaminti ir parduoti, jeigu tai pažemintų asmens garbę, orumą ar dalykinę reputaciją. LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.

140 Žr. „Vanna White v. Samsung Elecs. Am.“, Inc., 989 F. 2d 1512 (9th Cir. 1993), „Midler v. Ford Motor Co.“, 849 F.2d 460 (9th Cir. 1988).

141 Žr. „Steffi Graf Wins Case v. Microsoft“, AP NEWS, žiūrėta 2022 m. lapkričio 23 d., https://apnews.com/article/0cf8bc6052006588c21b22b4686119a. (Byloje nagrinėjamas ginčas kilo dėl to, kad internete pasirodė nuotraukos, kuriose žinomos tenisininkės Steffi Graf veidas buvo pridėtas prie kitos moters nuogo kūno nuotraukų. Teismas pasisakė, kad už tinklalapio turinį atsakinga „Microsoft Germany“ ir ji privalo užtikrinti, kad tos nuotraukos nebebūtų prieinamos, kitu atveju kompanijai bus skirta bauda.), Bertrand, *supra note,* 44: 127. (Autorius aprašo bylą, kurioje vaikinas į internetą įdeda nuogos buvusios savo merginos nuotraukas. Prancūzijos teismas vaikinui skyrė ne tik aštuonių mėnesių laisvės atėmimo bausmę, bet ir 25 000 frankų baudą.) Taip pat žr. „S. A. Multimania Prod. c. Madame L.“, No. 859, CA Versailles, 12eme ch., June 8, 2000; S.A. SPPI c. Societh Fox Media, No. R6: 01/04400, T.G.I. Paris, 3eme ch., May 29, 2002.

įžymybių nuotraukų, paskelbtų internete, nesivargina netgi imtis priemonių, kad tos nuotraukos būtų pašalintos iš viešosios erdvės[142].

Dar vienas pavyzdys sietinas su skirtingai suvokiamu privatumu darbo vietoje. Europoje asmuo net ir darbe gali tikėtis privatumo[143]. Tuo tarpu JAV, remiantis teismais, asmuo darbo vietoje tikėtis privatumo praktiškai negali[144].

Abiejose tradicijose egzistuoja teisės aktai, ginantys duomenų apsaugą[145], bet JAV duomenų apsaugos taikymo sritis reikšmingai siauresnė. Laikantis BDAR tam, kad duomenų tvarkymas būtų teisėtas, prieš pradedant rinkti duomenis, privaloma gauti duomenų subjekto sutikimą (arba duomenis tvarkyti kitu teisėtu tikslu[146]), o pagal JAV Kalifornijos vartotojų privatumo aktą (CCPA)[147] duomenims tvarkyti teisėtumas nėra būtina sąlyga[148].

Negalima būtų drąsiai teigti, jog privatumo suvokimas kontinentinėse valstybėse visiškai neturi nieko bendro su bendrąja teisės tradicija. Be abejo, abi jurisdikcijos viena iš kitos yra kažką pasiskolinusios[149]. Pvz., Europoje, panašiai kaip ir JAV, egzistuoja privatumo apsauga gyvenamojo būsto ribose[150]. Taip pat tiek JAV, tiek Europoje galima diskutuoti apie privatumo ir spaudos (saviraiškos) laisvės santykį[151]. Vadinasi, privatumo suvokimas kontinentinėje ir bendrosios teisės tradicijoje nėra absoliučiai skirtingas.

Šiame darbe atliekamam tyrimui ypač svarbūs privatumo apsaugos suvokimo skirtumai kontinentinės ir bendrosios teisės tradicijose, nes jie parodo dabartinių privatumo reguliavimo sprendimų kontekstą ir galimą kryptį ateityje. Kadangi Lietuva yra kontinentinės teisės tradicijos šalis ir šioje disertacijoje teikiamos rekomendacijos, tikėtina, padarys didžiausią įtaką Lietuvos

---

142 Whitman, *supra note,* 38: 1199–1200 (nagrinėjama JAV byla, kurią prieš bendrovę, užsiimančią nuotraukų, kuriose garsenybės nuogos, publikavimu, iškėlė Laura Schlessinger. Byloje teismas panaikino laikinąsias apsaugos priemones, įpareigojančias nutraukti tariamą pažeidimą – nuotraukų publikavimą atsakovo tinklalapyje, nes šios jau ir taip buvo plačiai pasklidusios internete. Ieškovė Laura Schlessinger galiausiai atsiėmė savo ieškinį byloje.).

143 Žr. „López Ribalda and Others v. Spain", No. 1874/13, 8567/13 (ECtHR [GC] 2019 m. spalio 17 d.).

144 Žr. „Thompson v. Johnson County Community College", 930 F. Supp. 501 (D. Kan. 1996)

145 Europoje galioja BDAR, o JAV ypač didelę reikšmę turi 2018 m. Kalifornijos vartotojų privatumo aktas (CCPA). Detalesnį šių teisės aktų palyginimą žr. Chander, Kaminski ir Mcgeveran, *supra note,* 39: 1733–1802.

146 BDAR, 6 straipsnio 1 dalis.

147 Kaip pavyzdį galima pateikti Kalifornijos vartotojų privatumo aktą (CCPA), nes jis laikytinas JAV iki tol neegzistavusios plačios vartotojų duomenų apsaugos „katalizatoriumi". Būtent juo remdamiesi beveik identišką duomenų apsaugą naujuose teisės aktuose užtikrino daugelis kitų Amerikos valstijų. Žr. Chander, Kaminski ir Mcgeveran, *supra note,* 39: 1733–1802.

148 *California Consumer Privacy Act of 2018* (CCPA); *California Civil Code* § 1798.100.

149 Whitman, *supra note,* 38: 1159.

150 Pvz., EŽTK 8 straipsnis užtikrina asmenų būsto neliečiamybę.

151 Saviraiškos laisvė JAV įtvirtinta pirmojoje konstitucijos pataisoje, o Europoje ją įtvirtina, pvz., EŽTK 10 straipsnis.

moksliniam diskursui ir teisiniam reguliavimui, platesnis istorinių privatumo ištakų kontekstas, aprėpiantis skirtingas Atlanto puses, taip pat leidžia „išfiltruoti“, t. y. aptikti, pernelyg amerikietiškas reguliavimo idėjas, kurios būtų sunkiai pritaikomos kontinentinės tradicijos šalyse.

1.4.5. Privatumas Lietuvoje

Nepaisant XVIII a. pabaigos nuotaikų, vyravusių Prancūzijoje revoliucijos metu, teisė į privatumą pirmąkart buvo įtvirtinta 1791 m. rugsėjo 3 d. priimtoje Prancūzijos konstitucijoje, o štai keliais mėnesiais anksčiau parengtoje Abiejų Tautų Respublikos Gegužės 3-osios Konstitucijoje privatumo apsauga nebuvo numatyta[152]. Privatumo apraiškų Lietuvoje radosi tik tarpukario metais. 1922 m. priimta Lietuvos Valstybės Konstitucija skelbė: „Piliečiui laiduojama korespondencijos ir susižinojimo paštu, telefonu, telegrafu paslaptis. Išimtis gali būti daroma įstatyme nurodytais atsitikimais“, taip pat nustatė: „Piliečio butas neliečiamas. Įeiti į butą ir daryti jame kratą galima tik įstatyme nurodytais atsitikimais ir tvarka“[153]. Analogiškos nuostatos galiojo ir 1928 m. Lietuvos Valstybės Konstitucijoje[154]. Šiuose dokumentuose privatumas neįtvirtinamas tiesiogiai, tačiau iš esmės saugomas per teisę į susižinojimo slaptumą ir teisę į būsto neliečiamumą. Šios teisės egzistuoja ir dabartinėje Lietuvos Respublikos Konstitucijoje[155].

1938 m., Lietuvoje jau galiojant diktatorinei valdžiai, piliečiai vis dar turėjo teisių, tačiau šios skambėjo kiek kitaip: „Valstybė saugo piliečių susižinojimo turinio paslaptį. Valstybė gali įstatymu tikrinti piliečių susižinojimo turinį, kiek tatai reikalinga Valstybės kovai su nusikaltimais“[156], taip pat skelbė: „Valstybė saugo piliečio buto neliečiamybę. Valstybė gali įstatymu aprėžti piliečio buto neliečiamybę, kiek tatai reikalinga Valstybės kovai su nusikaltimais“. Atlikus analizę matyti, kad vietoj žodžio „laiduojama“ 1938 m. Konstitucijoje vartojama frazė „valstybė saugo“, o vietoj frazės „įstatyme nurodytais atsitikimais“ įrašyta „valstybė gali tikrinti“ ir „valstybė gali aprėžti“. Šie pakeitimai reiškė, kad Lietuvos piliečiai privatumo apsaugos prieš valstybę tikėtis negalėjo. Spaudos laisvė tuo metu irgi buvo stipriai

---

152 „Gegužės 3-iosios Konstitucija | *Magnus Ducatus Lithuaniae*“, žiūrėta 2022 m. gruodžio 21 d., http://www.mdl.projektas.vu.lt/thesaurus/kaupiamos-kolekcijos/rankrasciai/geguzes-3-konstitucija/.

153 Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1922, „LR Konstitucija – 1922 m. Lietuvos Valstybės Konstitucija“, žiūrėta 2022 m. gruodžio 21 d., https://www.lrk.lt/lietuvos-konstitucijos-istorija/202-1922-m-lietuvos-valstybes-konstitucija.

154 Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1928, „1928_m._Lietuvos_Valstybės_Konstitucija.IH2105.pdf“, žiūrėta 2022 m. gruodžio 21 d., http://www.xn--altiniai-4wb.info/files/istorija/IH00/1928_m._Lietuvos_Valstyb%C4%97s_Konstitucija.IH2105.pdf.

155 Žr. LR Konstitucijos 22, 24 straipsnius.

156 Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1938, „Iš 1938 m. Lietuvos Konstitucijos“, http://www.xn--altiniai-4wb.info/files/istorija/IH00/I%C5%A1_1938_Lietuvos_Konstitucijos.IH2106.pdf.

ribojama[157], tad saugoti privatumą nuo nepagrįsto žiniasklaidos įsiveržimo realiai nebuvo reikalo.

Beveik analogišką apsaugą numatė ir sovietų okupacijos metais priimtos Lietuvos Tarybų Socialistinės Respublikos (LTSR) konstitucijos. Pagal jas Lietuvoje galiojo komunistinė santvarka. 1940 m. LTSR Konstitucijos 100 straipsnis skelbė: „Piliečių buto neliečiamybę ir susirašinėjimo slaptumą saugo įstatymas“[158]. O 1978 m. LTSR konstitucija papildomai saugojo ir „piliečių asmeninį gyvenimą“, „piliečių asmenybę“[159]. Vis dėlto kažin ar galima būtų teigti, jog tos nuostatos tame orveliškame pasaulyje teikė ką nors panašaus į šiuolaikinę privatumo apsaugą. Šių laikų demokratinių valstybių teisinė santvarka paremta teisiniu personalizmu, pagal kurį didžiausią reikšmę turi pripažinimas, jog visi asmenys (individai) savo vertybėmis, laisvėmis ir interesais yra vienodai vertingi ir šia prasme lygūs[160]. Todėl teisė į privatumą taip pat kyla iš asmens individualumo.

Tačiau komunistinėse santvarkose pagrindinis vaidmuo skiriamas ne individui, o kolektyvinei visuomenei – liaudžiai. Privataus gyvenimo slaptumas žmonėms neabejotinai buvo svarbus, pirmiausia vengiant valstybės įsikišimo, bet labiausiai iš baimės būti nubaustiems už veiklas, kurios prieštaravo sovietinei ideologijai. Kitaip tariant, žmonės tokioje visuomenėje vieni kitiems nenorėjo atskleisti savo privataus gyvenimo aplinkybių ne dėl to, kad jos galėtų patekti į žiniasklaidos priemones, o dėl baimės, kad jų elgesys gali netiesiogiai atskleisti jų „neištikimybę“ partijai ar kolektyvinėje visuomenėje „nederamą“ veiklą[161]. Tačiau teisė į privatų gyvenimą realiai nebuvo ginama, nepaisant žmonių noro apsaugoti savo privatumą nuo valstybės įsikišimo. Priešingai – stebėti, ką veikia kaimynai, ir skųsti valstybei už nusižengimus komunistinei ideologijai buvo netgi skatinama. Taigi, nors LTSR konstitucijose ir buvo skelbiama asmens ir jo būsto neliečiamybė, susirašinėjimo slaptumas, realiai privatumo apsauga sovietų okupuotoje Lietuvoje neegzistavo.

Atkūrus nepriklausomybę 1990 m. teisė į privatų gyvenimą Lietuvoje buvo įtvirtinta su dauguma jos vakarietiškų elementų. Kaip matyti iš dabartinės LR Konstitucijos 22 straipsnio, Lietuvoje garbė ir orumas, kaip ir Prancūzijoje bei Vokietijoje, yra teisės į privatų gyvenimą pamatas. Įstatymai ir teismas privalo užtikrinti, kad niekas nepatirtų savavališko ar neteisėto kišimosi asmeninį

---

157 Juozapas Vytas Urbonas, „Spaudos laisvė ir jos įtaka kuriant pilietinę visuomenę“, *Tiltai: humanitariniai ir socialiniai mokslai,* 1 (2005): 115–22.

158 *Lietuvos Tarybų Socialistinės Respublikos Konstitucija* (Pagrindinis Įstatymas). Vilnius: Lietuvos Liaudies Seimas, 1940-08-25.

159 Lietuvos Tarybų Socialistinės Respublikos Konstitucija (Pagrindinis įstatymas), LR Aukščiausioji Taryba, *Vyriausybės žinios,* 1978-01-01, 11–130.

160 Alfonsas Vaišvila, *Teisinis personalizmas: teorija ir metodas:(teisės sugrąžinimo visuomenei ideologija)* (Vilnius: Justitia, 2011).

161 Oksana Zabuzhko, „Publicity and Media under Communism and After: The Destruction of Privacy“, *Social Research* 69, 1 (2002): 35–47. (Straipsnyje rašoma, kaip sovietinė žiniasklaida formavo visuomenės suvokimą, kas derama, o kas ne. Pvz., tokie dalykai kaip seksualiniai santykiai, skyrybos ar dovanų priėmimas iš užsieniečių buvo suvokiami kaip tabu.).

ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą[162]. Lietuvos teisinėje sistemoje yra ir amerikietiško prado – tai privatumas namų ribose, kurį užtikrina Konstitucijos 23 straipsnis, numatantis, jog žmogaus būstas ir nuosavybė yra neliečiami[163].

Konstitucijoje aptartą teisę į privataus gyvenimo apsaugą detalizuoja CK, kurio 2.23 straipsnio 1 dalyje nurodoma: „Fizinio asmens privatus gyvenimas neliečiamas. Informacija apie asmens privatų gyvenimą gali būti skelbiama tik jo sutikimu". CK 2.23 straipsnio 2 dalyje nurodytas nebaigtinis sąrašas atvejų, kada teisė į privatų gyvenimą būtų pažeidžiama, tarp jų: 1) kai neteisėtai įeinama į asmens gyvenamąsias ir kitokias patalpas, aptvertą privačią teritoriją, 2) kai asmuo neteisėtai stebimas, 3) kai neteisėtai apieškomas asmuo ar jo turtas, 4) kai pažeidžiamas asmens telefoninio pokalbio, susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų konfidencialumas, 5) kai pažeidžiant įstatymų nustatytą tvarką paskelbiami duomenys apie asmens sveikatos būklę. CK 2.23 straipsnio 3 dalyje papildomai aiškinama, kad draudžiama ir pažeidžiant įstatymus rinkti informaciją apie asmens privatų gyvenimą bei surinktus duomenis skleisti, nebent, atsižvelgiant į asmens einamas pareigas ar padėtį visuomenėje, tokios informacijos skleidimas atitinka teisėtą ir pagrįstą visuomenės interesą tokią informaciją žinoti. CK komentare papildomai nurodoma, kad privatus yra toks žmogaus gyvenimas, kuris vyksta ne viešumoje, tai sritis, kur asmuo turi teisę būti paliktas vienas ir kur visuomenė neturi teisės kištis, t. y. vidiniai asmens šeimos santykiai, jo lytinis, dvasinis, religinis gyvenimas, sveikatos būklė[164].

Teisė į atvaizdą, kurią (jau anksčiau buvo aptarta) pirmiausia suformavo Prancūzijos teismai[165], pripažįstama ir Lietuvoje. Jurisprudencijoje laikomasi nuomonės, jog teisė į atvaizdą yra platesnės teisės į privatų gyvenimą dalis[166]. CK 2.22 straipsnio 1 dalis numato, kad „Fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu". Kaip jau minėta, tiek JAV, tiek kontinentinėse teisės šalyse, tarp jų ir Lietuvoje, atvaizdas gali turėti ekonominę vertę ir gali būti parduodamas. Vis dėlto, priešingai nei JAV, Lietuvoje net ir parduotos asmens nuotraukos negalima demonstruoti, atgaminti tokiu būdu, kuris pažemintų asmens garbę, orumą ar dalykinę reputaciją[167]. Toks suvokimas iš esmės kilęs tiek iš Prancūzijos teismų praktikos, tiek iš Vokietijos teisės teoretikų suformuotos „asmenybės" teisės[168] ir Lietuvoje įtvirtintas CK 1.1

---

162 LR Konstitucija, 1992 m. lapkričio 2 d., *Lietuvos aidas,* 1992, 220 (1992-11-10); *Valstybės žinios,* 1992, 33-1014 (1992-11-30), 22 straipsnis.

163 LR Konstitucija, 1992 m. lapkričio 2 d., *ibid.,* 24 straipsnis.

164 A. Bakanas ir kiti, *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys* (Vilnius: Justitia, 2002), 60.

165 Žr. disertacijos 1.4.1 poskyrį.

166 LAT Civilinių bylų skyriaus 2020 m. spalio 28 d. nutartis civilinėje byloje Nr. e3K-3-278-403/2020, *Teismų praktika* 54 (2020): 11–24.

167 LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.

168 Žr. disertacijos 1.4.1 poskyrį ir 1.4.2 poskyrį.

straipsnio 1 dalyje. Jame iš esmės skiriami trijų tipų santykiai, kuriuos reguliuoja civilinė teisė, t. y. 1) turtiniai, 2) asmeniniai neturtiniai, susiję su turtiniais, 3) asmeniniai neturtiniai, nesusijusius su turtiniais. Asmeniniai neturtiniai santykiai yra išskirtinis kontinentinės teisės tradicijų šalių darinys, tuo tarpu JAV egzistuoja tik turtiniai santykiai.

Turtiniai santykiai nuo neturtinių skiriasi savo objektu. Neturtinių objektas yra įgimta ar įgyta savybė, kuri neatsiejama nuo asmens, nes sudaro jo substanciją. Tokia savybė gali būti ir asmens atvaizdas, kuris apskritai suprantamas kaip neturtinių santykių, nesusijusių su turtiniais santykiais, objektas[169], tačiau, jeigu įgauna ekonominę vertę ir yra parduodamas, gali tapti ir asmeninių neturtinių santykių, susijusių su turtiniais santykiais objektu.

Privatumas Lietuvoje ginamas ne tik civilinės, bet ir administracinės bei baudžiamosios teisės normomis. Pvz., ANK 83 straipsnyje numatyta atsakomybė už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje[170]. BK XXIV išskiria nusikaltimus, kurie gali būti padaryti pažeidžiant asmens privatumą. Tarp jų, pvz., neteisėtas informacijos apie privatų asmens gyvenimą rinkimas ir neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas[171].

Taigi, kaip matyti, Lietuvoje asmenims suteikiama plati privatumo apsauga, paremta garbės ir orumo užtikrinimu, kokią rasime daugelyje kontinentinės teisės tradicijos šalių, nors egzistuoja ir JAV teisei būdinga apsauga nuo įsiveržimo į asmeninio būsto ribas. Lietuvoje, taip pat kaip ir Prancūzijoje bei Vokietijoje, egzistuoja su asmeniu neatsiejamai susijusios personalinės vertybės, kurių apsaugą nuo žeminančio panaudojimo Lietuvos teisė užtikrina, net jeigu jie perleidžiami tretiesiems asmenims. Kad privatumas Lietuvoje turi ypač didelę svarbą, rodo ir su jo pažeidimais susijusių tam tikrų veikų kriminalizavimas, ko nėra JAV teisinėje tradicijoje.

Prieš pradedant kitą tyrimo etapą, kuriame bus analizuojamas teisinis reguliavimas, susijęs su bepiločiais orlaiviais ir privatumu, pirmiausia vertėtų apsibrėžti, kokią grėsmę privačiam gyvenimui gali kelti bepiločių orlaivių naudojimas. Aiškesnį vaizdą leis susidaryti kitas disertacijos poskyris.

---

169 Egidijus Baranauskas ir kt., „Civilinė teisė. Bendroji dalis: vadovėlis aukštųjų mokyklų studentams“, (Vilnius: Mykolo Romerio universitetas, 2007), 48.

170 LR administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas. LR administracinių nusižengimų kodeksas, suvestinė (2022-11-01–2022-12-31) redakcija, LR Seimas, XII-1869, TAR, 2015-07-10, Nr. 11216.

171 LR baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas, suvestinė (2022-11-01–2022-12-31) redakcija, LR Seimas, VIII-1968, *Valstybės žinios,* 2000-10-25, Nr. 89-2741, XXIV skyrius, 167–168 straipsniai.

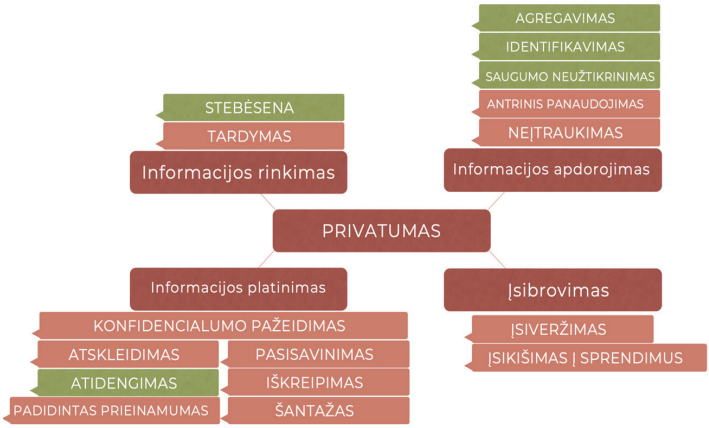
1.5. Privatumo pažeidimai, kuriuos gali sukelti bepiločių orlaivių naudojimas

Siekiant atskleisti teorines nedidelių bepiločių orlaivių naudojimo grėsmes privatumui, verta panagrinėti mokslinėje literatūroje aptariamas teisės į privatumą klasifikacijas. Teisės doktrinoje galima išskirti du pagrindinius būdus privatumui klasifikuoti: pagal pažeidžiamas vertybes arba pagal pažeidimus. Pirmąjį būdą išplėtojo Europos, antrąjį – JAV mokslininkai. Kontinentinėje Europoje privatumą į septynias vertybines kategorijas suskirstė R. Finn, D. Wrightas ir M. Friedewaldas[172]. JAV teisėje bene išsamiausią pažeidimų klasifikaciją sukūrė D. J. Solove'as[173].

Vertybinės privatumo klasifikacijos yra abstraktesnės, t. y. labiau tinka bendriems teisinio reguliavimo tikslams išsikelti, bet ne problemoms identifikuoti. Tuo tarpu pažeidimų klasifikacijos yra pragmatiškesnės, t. y. padeda vaizdingiau atkurti praktines situacijas, susidarančias dėl bepiločių orlaivių naudojimo, todėl aiškiau parodo, kokią grėsmę nedidelių bepiločių orlaivių naudojimas gali kelti privatumui. Siekiant nedviprasmiškai atskleisti bepiločių orlaivių keliamą grėsmę privatumui, šioje disertacijos dalyje bus vadovaujamasi D. J. Solove'o sukurta pažeidimų klasifikacija, kuri pateikiama 1 schemoje.

Vadovaujantis šia klasifikacija bus identifikuoti pažeidimai, kurie gali kilti vis didėjant nedidelių bepiločių orlaivių pritaikymo galimybėms. Žinoma, bepiločiai orlaiviai nesukelia absoliučiai visų klasifikacijoje nurodytų pažeidimų, todėl daugiau dėmesio skiriama toms grėsmėms, kurios labiausiai siejasi su bepiločių orlaivių naudojimu, – t. y. stebėsena, agregavimas, identifikavimas, saugumo neužtikrinimas ir atidengimas (1 schemoje pažymėta žaliai).

1 schema. Privatumo pažeidimų klasifikacija



172 Finn, Wright ir Friedewald, *supra note,* 37: 3–32.
173 Solove, „A Taxonomy of Privacy", *supra note,* 36: 477–564.

1.5.1. Stebėsena

Nedideliems bepiločiams orlaiviams būdingas skrydžio kontrolės paprastumas ir vaizdo fiksavimas. Tikėtina, jog technologijoms tobulėjant maži bepiločiai orlaiviai per didelį atstumą, o vabzdžio dydžio – iš labai arti galės įrašyti ne tik vaizdą, bet ir garsą, fiksuoti šilumos pakitimus aplinkoje, aptikti cheminius pėdsakus[174], nustatyti bevielį duomenų srautą[175]. Dėl šių techninių galimybių bepiločiai orlaiviai privatumo teisės kontekste pirmiausia yra informacijos rinkimo priemonės, todėl patenka į 1 schemoje įvardytą *informacijos rinkimo* pažeidimų kategoriją. Iš dviejų šios kategorijos privatumo pažeidimo rūšių bepiločiams orlaiviams tinka vienas – *stebėsena*. Jie gali būti naudojami žmonėms stebėti (darant vaizdo ar garso įrašus), kurie apie tai nežino arba tik numano. Tiesa, šiuo metu, kai technologinės galimybės leidžia valdyti bepiločius orlaivius daugiausia tik nuotoliniu būdu, plataus masto sekimas pareikalautų ypač didelių žmogiškųjų išteklių, tačiau, vis didėjant skraidančių pagalbininkų autonomijai, galimybė pasirinktą asmenį stebėti nuolatos galiausiai taps reali.

Šiais laikais stebėseną gali vykdyti ne tik valstybės, bet ir didelę galią rinkoje turinčios privačios kompanijos. Abi subjektų grupės pavojingos ir tarpusavyje susijusios, abi turi tam reikalingus išteklius, tačiau tiktai valstybėms suteikti įgaliojimai, leidžiantys vykdyti sistemingą ir plataus masto stebėseną. Skiriasi ir šių subjektų motyvacija, jei privačių įmonių vykdomos stebėsenos tikslas yra padidinti parduodamų produktų ar paslaugų paklausą, tai valstybės surinktą informaciją gali panaudoti kur kas ambicingesniems tikslams ir sukelti didesnių neigiamų pasekmių[176]. Negana to, valstybės gali naudotis privačių subjektų sukurta stebėsenos infrastruktūra teisės aktuose nustatydamos reikalavimą kaupti surinktą informaciją ir, esant reikalui, suteikti prieigą valdžios institucijoms[177], taip pat valstybė gali pareikalauti surinktą informaciją iš karto perduoti valdžios institucijoms. Kita vertus, ar blogai, kad valstybė kaupia informaciją siekdama apsaugoti savo piliečius?

---

174 Randy Rieland, „Teaching Drones to Sniff Out Toxic Air“, *Smithsonian Magazine,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.smithsonianmag.com/innovation/teaching-drones-sniff-out-toxic-air-180970231/.

175 Vienas iš mažiau žinomų faktų apie stebėjimui ir kariniams tikslams naudojamus bepiločius orlaivius yra tas, kad be ginklų, kamerų ir kitų jutiklių jie aprūpinti dar ir įrenginiu, vadinamu „Air Handler“, kuris gali fiksuoti aplinkinį belaidį duomenų srautą. Žr. Mark Andrejevic ir Kelly Gates, „Big Data Surveillance: Introduction“, *Surveillance & Society* 12, 2 (2014 m. gegužės 9 d.), 185–196, https://doi.org/10.24908/ss.v12i2.5242.

176 Užtenka prisiminti ambicingą nacistinės Vokietijos siekį sukurti Adolfo Hitlerio valdomą naują, harmoningą visuomenę. Siekiant šio tikslo buvo pražudyti beveik šeši milijonai žydų.

177 Pvz., Lietuvos elektroninių ryšių įstatymas leidžia elektroninių ryšių teikėjams kaupti telefoninių pokalbių įrašus ir bet kokius kitus duomenis apie elektroninių ryšių vartotojus siekiant užtikrinti, kad šie duomenys vėliau būtų prieinami valstybei saugumo tikslais, žr. LR elektroninių ryšių įstatymas (suvestinė redakcija nuo 2020-01-17), *Žin.* (2004, Nr. 69-2382), 65 straipsnio 2 dalis.

Argi nėra verta atiduoti dalį savo privatumo dėl saugumo? Ar stebėsena gali būti laikoma privatumo pažeidimu, jeigu valstybė tai daro siekdama apsaugoti savo piliečius nuo sunkių nusikaltimų?

Kiekviena valstybė tam tikru mastu vykdo žvalgybinę veiklą, o jos mastas paprastai koreliuoja su valstybės dydžiu ir ekonominiu pajėgumu – kuo didesnė ir turtingesnė valstybė, tuo platesnis jos žvalgybos tinklas. Pavyzdžiui, Edwardo Snowdeno atskleistas skandalas[178] parodė, jog didžiausios ir galingiausios pasaulio valstybės gali į asmenų gyvenimus įsibrauti net ir pačiomis netikėčiausiomis priemonėmis. Nors tokio pobūdžio sekimas daugeliui individų kelia diskomfortą, valstybės dažnai pateikia argumentą: „nėra ko bijoti, jei neturi ko slėpti."[179]. Ir iš tiesų, kodėl valstybės vykdoma stebėsena turėtų būti laikoma privatumo pažeidimu, jeigu dauguma surinktos informacijos nėra jautri, informacija atskleidžiama tik tuo atveju, jeigu išaiškinamas nusikaltimas, o asmenys, bandę nuslėpti nusikalstamą veiką, neturi jokios pagrįstos teisės išsaugoti nusikalstamos veikos privatumą. Verta pažymėti, kad ateityje bepiločiai orlaiviai informaciją rinks vis labiau autonomiškai, o surinktus duomenis analizuos pažangios kompiuterinės sistemos. Todėl, jei asmuo nevykdys jokios neteisėtos veiklos, dirbtinio intelekto valdomos sistemos, neužfiksavusios įtartinų veiksmų, tiesiog praleis surinktą informaciją, o vizualiniai ar kitokio pobūdžio duomenys niekada nepasieks valstybės institucijų. Remiantis šia logika, teisės besilaikantiems piliečiams nerimauti dėl savo privatumo pagrindo nėra, nes valstybės žvalgybinių struktūrų tikslas – stebėti ir identifikuoti ne teisėtai veikiančius visuomenės narius, bet tuos, kurie vykdo nusikalstamas veikas.

Vis dėlto, populiarus valstybių argumentas, jog „nėra ko bijoti, jeigu neturi, ko slėpti", suponuoja supaprastintą ir trumparegišką privatumo sampratą, redukuojančią šią sąvoką iki vienintelio aspekto – siekio nuslėpti neteisėtą ar moraliai nepriimtiną veiklą nuo trečiųjų asmenų. Tačiau privatumas yra daugialypė socialinė vertybė, apimanti įvairius esminius elementus, kurie atlieka reikšmingą funkciją visuomenėje. Todėl vien siekis nuslėpti „kažką blogo" tėra menka privatumo koncepcijos dalis. Nors nuolatinė asmenų stebėsena gali būti traktuojama kaip privatumo pažeidimas, pats stebėjimo poveikis žmonių elgesiui ne visada yra neigiamas. Pavyzdžiui, viešųjų erdvių stebėjimas vaizdo kameromis (CCTV) gali skatinti socialiai atsakingesnį elgesį ir mažinti nusikalstamumo riziką. Tačiau pernelyg išplėtotas socialinės kontrolės mechanizmas, ypač kai stebėsena vykdoma pasitelkiant vabzdžio dydžio bepiločius orlaivius, galinčius fiksuoti vaizdą ir garsą iš itin arti arba dideliu atstumu, išlikdami nematomi ir negirdimi, gali turėti neigiamą poveikį individų savijautai bei elgesiui. Toks slaptas ir visapusiškas stebėjimas gali

178 Edward Snowden, buvęs CŽV darbuotojas, 2013 m. birželio mėnesį žiniasklaidai paviešino išsamią informaciją apie Amerikos žvalgybos vykdytą išsamų interneto ir telefonų stebėjimą, žr. „How the US Spy Scandal Unravelled", *BBC News,* 2014 m. sausio 17 d., posk. US & Canada, https://www.bbc.com/news/world-us-canada-23123964.

179 Solove, „I've Got Nothing to Hide and Other Misunderstandings of Privacy 2007 Editor's Symposium", *supra note,* 36: 748.

sumažinti asmens laisvės pojūtį, slopinti kūrybiškumą, riboti saviraišką bei skatinti savicenzūrą, nes žmonės, žinodami, kad yra nuolat stebimi, linkę labiau konformistiškai prisitaikyti prie dominuojančių socialinių normų[180].

Mokslininkai šį reiškinį, kai visuomenė dėl stebėsenos tampa labiau savidisciplinuota ir suvaržyta, vadina atšalimo arba *panoptiniu efektu*[181]. Tai reiškia, kad nuolatinės kontrolės baimė sukuria situaciją, kurioje žmonės keičia savo elgesį, net jei realios grėsmės ar stebėjimo fakto nėra, taip sukurdami nuolat veikiančią savikontrolės sistemą, grindžiamą ne tik baime, bet ir vidiniu spaudimu laikytis visuotinai priimtų normų.

Slaptai vykdoma stebėsena pažeidžia asmens teisę į privatumą ne tik tada, kai individas yra privačioje aplinkoje, pavyzdžiui, savo gyvenamajame būste, asmeniniame žemės sklype ar kitoje jam priklausančioje erdvėje, bet ir tuomet, kai jis yra viešojoje erdvėje, tačiau turi pagrįstą lūkestį, jog nėra stebimas. Tokie atvejai apima situacijas, kai asmuo ilsisi atokesniame viešo parko kampelyje ar dalyvauja triukšmingame sporto renginyje tarp daugybės kitų žmonių. Be abejo, būdamas viešojoje erdvėje, individas gali tikėtis, kad atsitiktinai gali patekti į kitų asmenų darytas nuotraukas ar vaizdo įrašus, kuriuose fiksuojama ir daugiau žmonių. Tačiau jis neturėtų pagrįstai numanyti, kad yra tikslingai stebimas, jo atvaizdas fiksuojamas iš arti ar įrašinėjamas jo pokalbis naudojant kryptinius mikrofonus[182]. Nors įprasta manyti, kad viešoje vietoje privatumo lūkestis yra mažesnis[183], šiuolaikinės bepiločių orlaivių technologijos leidžia vykdyti tokio masto sekimą, kuris gali reikšmingai pažeisti asmens teisę į privatumą net ir viešojoje erdvėje. Iki šiol nuolatinė individuali stebėsena viešose vietose buvo sudėtinga dėl didelių techninių ir finansinių išteklių poreikio. Tačiau bepiločių orlaivių plėtra šias kliūtis eliminuoja – šie įrenginiai suteikia galimybę nuotoliniu būdu sekti asmenį iš įvairių kampų ir reikšmingai sumažina sistemingos bei ilgalaikės stebėsenos kaštus. Svarbu pabrėžti, kad nuolatinė stebėsena viešojoje erdvėje gali pažeisti asmens teisę į privatumą net labiau nei stebėjimas jo privačioje aplinkoje. Tai, kur individas lankosi, su kuo bendrauja ir kaip elgiasi viešosiose vietose, gali atskleisti daug daugiau apie jo

---

180 Solove, „A Taxonomy of Privacy," *supra note,* 36: 493–494.

181 Terminas panoptinis yra kilęs iš Jeremy'io Benthamo aprašyto utopinio kalėjimo, vadinamo Panoptikumu, kurio architektūriniai sprendimai sudarė galimybę stebėti kalinius, tačiau šie nežinojo, kad bet kada *gali* būti stebimi. Jeremy Bentham, *Panopticon Or the Inspection House* (T. Payne, 1791).

182 Clarke, „The regulation of civilian drones' impacts on behavioural privacy", *supra note,* 28: 288.

183 Pvz., LR CK 2.22 straipsnio 1 dalis numato, kad „fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu", tačiau to paties straipsnio 2 dalis numato išimtį, kad „tais atvejais, kai fotografuojama (filmuojama) viešoje vietoje, asmens sutikimo nereikia", žr. LR civilinis kodeksas (suvestinė redakcija nuo 2025-01-15 iki 2026-03-31), *Žin.* (2000-09-06, Nr. 74-2262). Analogišką problemą D. Solove'as įžvelgia ir JAV, kaip yra reglamentuojamas privatumas, Solove, „A Taxonomy of Privacy", *supra note,* 36: 498.

gyvenimo būdą, socialinius ryšius, politines pažiūras ar religinius įsitikinimus nei stebėsena namų aplinkoje. Tokiu būdu bepiločių orlaivių technologijos išplečia valstybių ir kitų subjektų galimybes stebėti asmenis, keldamos naujus iššūkius privatumo apsaugos teisiniam reguliavimui ir asmeninių laisvių užtikrinimui.

Privatumas gali būti pažeistas ir tada, kai konkretus asmuo nėra sistemiškai sekamas ir nėra pagrindinis sekimo objektas. Šiuolaikinės stebėjimo technologijos leidžia kaupti didžiulius informacijos srautus apie bet ką, nesiorientuojant į konkrečius individus, o sukauptus duomenis saugoti neribotą laiką. Tokiu būdu nebereikia aktyviai sekti atskirų asmenų – pakanka nuolat rinkti ir archyvuoti visų stebimų asmenų duomenis, kurie prireikus gali būti analizuojami bei panaudojami pagal situacijos poreikius[184]. Tokio masto surinktos informacijos apdorojimui būtina pasitelkti pažangias kompiuterines programas, kurios, naudodamos iš anksto suprogramuotus algoritmus, gali nustatyti veiksmų modelius, atpažinti veidus, analizuoti specifinius žodžius ar kitus duomenų aspektus. Nors surinkta informacija gali būti neviešinama, ji išlieka prieinama tam tikroms institucijoms ar subjektams ir, esant poreikiui, gali būti panaudota prieš stebimus asmenis siekiant įgyti strateginį pranašumą.

Kaip privatumo apsauga gali būti pažeidžiama, kai masiškai kaupiami ir sistemingai apdorojami dideli informacijos kiekiai, išsamiau nagrinėjama tolesniame poskyryje, kuriame analizuojamas privatumo pažeidimo mechanizmas, kylantis dėl vis didesnio mažųjų bepiločių orlaivių prieinamumo, – kitaip tariant, informacijos agregavimas.

1.5.2. Agregavimas

Bepiločiai orlaiviai apdoroja surinktą informaciją naudodami programinę įrangą, t. y. informaciją perkelia į laikmeną, perduoda duomenis duomenų ryšiu, atkuria filmuojamą vaizdą valdymo pulto ekrane ir pan. Tad bepiločiais orlaiviais įmanoma vykdyti privatumo pažeidimus, įvardytus D. J. Solove'o klasifikacijos *informacijos apdorojimo kategorijoje*[185].

Anksčiau dėl praktinių apribojimų milijonų žmonių judėjimo dideliame mieste stebėjimas realiuoju laiku buvo neįmanomas. Tačiau šiandien pažangios technologijos, įskaitant bepiločius orlaivius, leidžia atskleisti naudingas, tačiau iš pirmo žvilgsnio nepastebimas žmonių elgsenos struktūras. Žmogus fiziškai nepajėgtų apdoroti tokio didelio duomenų kiekio, tačiau bepiločiai orlaiviai gali surinkti milžiniškus informacijos srautus, kurie vėliau analizuojami pasitelkiant pažangią programinę įrangą. Šis procesas, kai skirtingi duomenų fragmentai sujungiami į vientisą visumą ir gali kelti grėsmę privatumui, vadinamas *agregavimu*..

Kaip ir stebėsena, agregavimas yra būdas surinkti informaciją apie žmones, tačiau netiesioginiu būdu – apdorojant jau surinktą informaciją. Bepiločiai orlaiviai

184 Andrejevic ir Gates, „Big Data Surveillance", *supra note,* 179: 185.
185 Žr. 1 schemą.

informacijos apdorojimo procese dalyvauja labai nedaug, nes jų pagrindinė užduotis yra informaciją surinkti ir perduoti į duomenų bazę, kurioje programinė įranga toliau atlieka rūšiavimo ir interpretavimo darbus. Vis dėlto bepiločiai prie tokio pažeidimo prisideda reikšmingai, nes prisideda prie oportunistinio, visur esančio informacijos rinkimo[186]. Tokio plataus masto informacijos rinkimas ir apdorojimas, kurio tikslas ne ką nors sužinoti apie konkretų asmenį, bet veikiau surinkti kuo daugiau ir bet kokios informacijos apie visus įmanomus asmenis, vadinamas terminu *didieji duomenys* (angl. *big data*). Įvairių jutiklių turintys bepiločiai orlaiviai yra pajėgūs fiksuoti ne tik daugybę vaizdų, garsų, bet ir visur sklindantį duomenų ryšį (belaidį, „Bluetooth“, GPS ir pan.), todėl ateityje duomenų bazės, kuriose surinktus duomenis bus galima agreguoti, kaups informaciją ne tik apie tai, ką mes darome elektroninėje erdvėje[187], bet ir apie tai, kaip mes elgiamės realiame gyvenime. Surinktus duomenis bus galima panaudoti geriems tikslams, pvz., įvertinti ligų paplitimą, sekti verslo tendencijas, išaiškinti organizuotą nusikalstamumą, analizuoti interneto srautą bei įvairias prognozes nuo orų iki finansinių rinkų[188].

Vis dėlto bepiločių orlaivių derinimas su milžiniškomis duomenų bazėmis bei agregavimo programine įranga didžiųjų duomenų valdytojams gali suteikti dingsčių savo padėtimi piktnaudžiauti. Agregavimas gali kelti grėsmių privatumui, nes apie asmenį bus įmanoma gauti tokios informacijos, kurios šis atskleisti nesitikėjo. Nors asmuo kasdien įsitraukdamas į įvairias veiklas šiek tiek palieka savo elgesio duomenų, bet jis viliasi, kad tai mažai ką gali pasakyti apie jo asmeninį gyvenimą. Tačiau, kai visos dalelės bus konsoliduotos, atlikus agregavimą apie asmens gyvenimą bus sužinota kur kas daugiau, negu šis galėtų įsivaizduoti[189].

---

186 Andrejevic ir Gates, „Big Data Surveillance“, *supra note,* 179: 185.

187 Tokios kompanijos kaip „Google“ ar „Facebook“ jau dabar yra sukaupusios milžiniškus asmens duomenų kiekius, kurie leidžia nuspėti žmonių elgesio struktūras. Žr. Ben Popken, „Google Sells the Future, Powered by Your Personal Data“, *NBC News,* 2018 m. gegužės 10 d., https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501.

188 Andrejevic ir Gates, „Big Data Surveillance“, *supra note,* 179: 186.

189 Kashmir Hill, „How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did“, *Forbes,* žiūrėta 2022 m. lapkričio 25 d., https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/. (Pvz., JAV prekybos tinklas „Target“ iš klientės pirkinių krepšelio yra nuspėjęs, kad ši laukiasi. Kadangi JAV gimimo įrašai dažniausiai yra vieši, „Target“ ir kiti parduotuvių tinklai šeimoms, kurios neseniai buvo susilaukusios vaiko, siųsdavo kuponus ir reklamas kūdikių prekėms įsigyti. Tačiau „Target“ nusprendė šeimas pasiekti pirmiau, kol moteris dar laukiasi, ir aplenkti savo konkurentus. Vienintelis klausimas buvo, kaip nustatyti, kad moteris yra nėščia. Padėti galėjo duomenys, kuriuos kompanija kaupė milžiniškoje vidinėje duomenų bazėje apie klientų įsigytas prekes. Parduotuvių tinklas, palyginęs įsigyjamų pirkinių duomenis su viešais gimimo įrašais, nustatė pagrindines prekes, kurias šeimos dažniausiai įsigijo dar prieš gimstant vaikui, pvz., bekvapis kūdikių kremas, kalcio papildai ir dezinfekcinės priemonės. Šį standartinį nėščios moters profilį pritaikė praktiškai. Kaskart, kai moteris įsigydavo produktų, esančių sąraše, „Target“ jai skirdavo aukštą prognozuojamo nėštumo balą ir siųsdavo su kūdikiais susijusių produktų reklamas bei kuponus. Kompanijai vykdant tokią reklamos strategiją po kelių mėnesių į vieną iš parduotuvių atėjęs vyras pasiskundė, kad „Target“ jo penkiolikmetei dukrai siunčia su kūdikiais susijusius kuponus, ir įpykęs klausė, ar parduotuvių tinklas stengiasi įtikinti jo dukrą, kad ši pastotų. Su vyru bendravęs vadybininkas labai atsiprašė dėl nesusipratimo ir vyras išėjo. Netrukus po incidento vadybininkas paskambino vyrui, kad jo atsiprašytų, tačiau prieš tai pasipiktinęs tėvas šį kartą jau buvo susigėdęs ir pats atsiprašinėjo vadybininko. Paaiškėjo, jog vyras pasikalbėjo su dukra ir sužinojo, kad ši iš tikrųjų buvo nėščia, t. y. „Target“ tai sužinojo pirmiau negu merginos tėvas.)

Kita agregavimo keliama grėsmė – tai galios pasiskirstymas visuomenėje. Įprasta valdžios institucijų vykdoma stebėsena būna selektyvi, t. y. dažniausiai būna sekamas konkretus asmuo (įtariamasis), galimai padaręs kokį nors nusikaltimą. Didieji duomenys visiškai pakeičia stebimojo (įtariamojo) sąvoką, nes stebimi ne konkretūs individai ar įvykiai, o duomenyse slypinčios elgesio struktūros[190]. Didžiųjų duomenų stebėjimo esmė – surinkti kiek įmanoma daugiau informacijos, o vėliau ją išrūšiuoti pagal naudingumą. Kaip teigia Markas Andrejevicius ir Kelly Gates, naudojantis didžiaisiais duomenimis dažniausiai nėra bandoma paaiškinti ar suprasti pasaulį, kurį jie užfiksuoja. Tokio stebėjimo tikslas yra *įsikišti* į pasaulį per elgesio struktūras, kurias gali pastebėti tiktai tie, kas turi priėjimą ir galimybę didžiuosius duomenis apdoroti. Didžiųjų duomenų pasaulyje nebelieka jokio skirtumo tarp įtariamųjų ir neįtariamųjų, nes tam, kad tarp jų būtų galima įžiūrėti reikšmingesnių skirtumų, reikia informacija tiek apie vienus, tiek apie kitus[191]. Kaupiant informaciją tokiu būdu, pasak J. Packerio, visa realybė yra išverčiama į skaitmeninius duomenis, dėl to ir visas pasaulis per skaitmeninę manipuliaciją gali būti transformuojamas[192]. Jeigu vien socialiniuose tinkluose surinkta informacija gali lemti JAV prezidento rinkimų rezultatus[193], socialinės kontrolės mastas, kuris gali būti pasiektas informaciją renkant bepiločiais orlaiviais, tikriausiai mažai skirtųsi nuo George Orwello vaizduojamo totalitarizmo[194]. Kevino D. Haggerty'o ir Richardo V. Ericsono manymu, šiuo metu stebėjimo technologijų galimybės netgi pranoko G. Orwello distopinę viziją. Pirma, dėl to, kad G. Orwello romane nuolatinį stebėjimą vykdė tik valstybės institucijos, o dabar visuomenę masiškai stebi ne tik valstybė, bet ir nevalstybinės institucijos. Antra, dėl to, kad G. Orwello prognozėse „proliai" turėtų būti atleidžiami nuo stebėjimo, bet šiais laikais, panašu, visuomenė yra stebima be išimčių[195].

Dar viena agregavimo keliama grėsmė atsiranda dėl surinktų duomenų patikimumo. Didieji duomenys neišvengiamai priklauso nuo infrastruktūros, kuri sudaro sąlygas informaciją rinkti ir apdoroti. Bet kokį sistemos netobulumą kompensuoja surinktų duomenų kiekis, t. y. kuo daugiau informacijos duomenų bazėje, tuo patikimesnės išvados. Svarbiausia šio proceso stadija yra informacijos surinkimas,

---

190 Andrejevic ir Gates, „Big Data Surveillance," *supra note,* 179: 190.

191 *Ibid.*

192 Jeremy Packer, „Epistemology Not Ideology OR Why We Need New Germans", *Communication and Critical/Cultural Studies* 10, 2–3 (2013 m. rugsėjo mėn.): 298, https://doi.org/10.1080/14791420.2013.806154.

193 Turimas omenyje „Cambridge Analytica" skandalas, žr. „What Did Cambridge Analytica Do During The 2016 Election?", *NPR.org,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election.

194 George Orwell ir A. M. Heath, *Animal farm and 1984* (Houghton Mifflin Harcourt, 2003).

195 Kevin D. Haggerty, Richard V. Ericson, „The Surveillant Assemblage", *British Journal of Sociology* 51, 4 (2000 m. gruodžio 1 d.): 606, https://doi.org/10.1080/00071310020015280.

nes nuo surinktų duomenų kiekio ir objektyvumo priklauso, kiek bus patikimos algoritmų sugeneruotos išvados. Duomenų rinkimą itin praplečia bepiločių orlaivių technologija, nes ji padeda informaciją rinkti realioje erdvėje iš daugelio skirtingų kampų. Tačiau, net ir bepiločiais orlaiviais padidinus surenkamos informacijos kiekį, nėra garantijos, kad surinkti duomenys bus išsamūs ar reprezentatyvūs. Duomenys gali tapti šališki, pvz., dėl neobjektyvaus rūšiavimo algoritmo[196]. Vienintelis būdas užtikrinti duomenų patikimumą – visiškai atkurti pasaulį įrašytų duomenų forma ir rinkti informaciją apie patį duomenų rinkimo procesą, tai kartoti iki begalybės[197]. Kitaip tariant, kad ir kiek bandytume duomenų užfiksuoti, šie duomenys būtų tiktai nedidelis realybės mėginys, kuris ne visuomet ją atspindėtų. Užfiksuoti duomenys iš prigimties nėra reikšmingi, todėl algoritmai tam tikrais atvejais gali atrasti įsivaizduojamas veiksmų sekas, nors koreliacijos tarp kintamųjų įrašytuose duomenyse gali būti visiškai atsitiktinės ir tarpusavyje neturėti jokio priežastinio ryšio[198]. Šis sistemos netobulumas kelia grėsmę privatumui, nes sukuria terpę klaidingai individų elgesio interpretacijai.

Dennisas D. Hirschas kaip pavyzdį pateikia duomenų analitikų ir sveikatos priežiūros specialistų bendrą iniciatyvą, kurios tikslas – visuomenėje atpažinti individus, kurių rizika susirgti diabetu didesnė, ir jiems suteikti prevencinę priežiūrą[199]. Viena vertus, tokie duomenys medikų rankose galėtų išgelbėti daugybę gyvybių. Kita vertus, jeigu prie šių duomenų galėtų prieiti ir bankai ar kitos didelės korporacijos, ta pati informacija apribotų individų galimybę susirasti darbą, gauti paskolą, apsidrausti ar nusipirkti būstą. Tikėtina, jog tobulėjant duomenų agregavimo technologijoms, vis daugiau verslų sprendimus priims vadovaudamiesi didžiųjų duomenų programų suformuotomis išvadomis[200]. Negana to, tikėtina, jog verslo subjektai, naudojantys nuspėjamuosius modelius, ar net valstybės tokias praktikas laikys griežtai konfidencialiomis, tad individai nė neįtars, kas gali būti įrašyta jų „byloje“. Akivaizdu, jog agregavimo technologijų suformuoti spėjimai vis daugiau lems asmenų gyvenimo galimybes, todėl net ir menkiausia klaidinga algoritmo interpretacija galėtų turėti pragaištingų pasekmių žmogui susirasti darbą, užsidirbti, keliauti, mokytis ir pan[201].

---

196 Kelly A. Gates, „Our biometric future“, *Our Biometric Future* (New York University Press, 2011).

197 Andrejevic ir Gates, „Big Data Surveillance,“ *supra note,* 179: 190–191.

198 Rob Kitchin, „Big Data, New Epistemologies and Paradigm Shifts“, *Big Data & Society* 1, Nr. 1 (2014 m. liepos 10 d.), p. 5, https://doi.org/10.1177/2053951714528481.

199 NYU Web Communications, „Independence Blue Cross, NYU, NYU Langone Medical Center Collaborate to Detect Early Diabetes“, žiūrėta 2019 m. balandžio 4 d., http://www.nyu.edu/content/nyu/en/about/news-publications/news/2013/april/independence-blue-cross-nyu-nyu-langone-medical-center-collaborate-to-detect-early-diabetes.

200 Dennis D. Hirsch „That's unfair-or is it: Big data, discrimination and the FTC's unfairness authority“, Ky, LJ 103 (2014): 345.

201 *Ibid.,* 346.

Agregavimas yra bevertis, jeigu nėra duomenų, kuriuos galima būtų analizuoti ir interpretuoti. Nors bepiločiai orlaiviai informacijos analizės ir interpretavimo procese praktiškai nedalyvauja, prie šio agregavimo pažeidimo prisideda įgalindami oportunistinį, visur esantį informacijos rinkimą. Agregavimą derinti su milžinišku informacijos kiekiu gali būti labai pavojinga. Kaip jau buvo minėta, agregavimas sukuria neproporcingą galios pusiausvyrą visuomenėje, kur viską kontroliuoti gali tie, kurie valdo informaciją. Net ir nepiktnaudžiaujant surinkta informacija, agregavimo programinės įrangos užfiksuotos elgesio struktūros ne visada gali atitikti tiesą, o tai gali sukelti nepagrįstų išankstinių nusistatymų, nulemsiančių žmonių gyvenimus. Tačiau net ir agregavimas nebūtų toks pavojingas, jeigu ne dar vienas pažeidimas, kuris taip pat suteikia galimybę atpažinti stebimus individus. Toliau bus kalbama apie *identifikavimą.*

1.5.3. Identifikavimas

Identifikavimas – tai tikrosios informacijos apie individą atskleidimas, kuris leidžia skaitmeninėse duomenų bazėse esančią informaciją pritaikyti konkrečiam asmeniui. Kitaip tariant, identifikavimas yra informacijos susiejimas su konkrečiais individais[202]. Viena vertus, identifikavimas turi daug privalumų. Patikimai nustatoma asmens tapatybė palengvina sandorių sudarymą, padeda užtikrinti banko operacijų skaidrumą ir saugumą, palaikyti viešąjį saugumą, nustatyti nusikaltimą padariusius asmenis ir pan.

Kita vertus, yra ir neigiama identifikavimo pusė. Tapatybės nustatymas individams užkrauna informacinį bagažą, kuris jų atžvilgiu gali sukelti išankstinį nusistatymą. Pvz., vienoje EŽTT byloje Prancūzijos pilietis norėjo savo asmens dokumentuose (tapatybės kortelėje, pase ir balsavimo kortelėje) pasikeisti lytį, nes buvo chirurginiu būdu pasikeitęs lytį (iš vyriškos į moterišką), tačiau Prancūzijos teisinė sistema tokios galimybės nenumatė. Kadangi asmens kode atsispindi asmens lytis ir tai atskleidžiama daugeliui institucijų, tai asmeniui neleido paslėpti fakto, kad jis yra transseksualas. Teismas pripažino, kad apribojimas pasikeisti lytį asmens dokumentuose pažeidė teisę į privatų gyvenimą[203]. Manytina, jog ši byla yra vienas iš akivaizdžių pavyzdžių, kada identifikavimas susiedamas individus su praeitimi, nuo kurios jie nori pabėgti, slopina jų galimybę keistis ir trukdo jų savarankiškam vystymuisi[204].

Indentifikavimas padidina valstybės galią individų atžvilgiu. Daugelyje valstybių biometriniai duomenys, tokie kaip asmens kodas, vardas, pavardė, žmonėms yra suteikiami nuo pat gimimo. Jų neturint būtų sudėtinga gyventi visuomenėje, nes identifikuoti save jau privaloma kone kiekviename žingsnyje – kai norima atsidaryti banko sąskaitą, jungiantis prie elektroninės

202 Solove, „A Taxonomy of Privacy“, *supra note,* 36: 511.
203 „B. v. France“, No. 57/1990/248/319 (European Court of Human Rights 1992 m. sausio 24 d.).
204 Solove, „A Taxonomy of Privacy“, *supra note,* 36: 514.

bankininkystės paskyros, atliekant notarinius sandorius, keliaujant į užsienio valstybę ir pan. Surinktus duomenis valstybės gali panaudoti ne tik savo piliečių apsaugai ar pinigų plovimo, terorizmo, nusikaltimų prevencijai, bet ir siekdamos apriboti žmonių judėjimą, slopinti nepasitenkinimą valstybine santvarka, izoliuoti tam tikras visuomenės grupes. R. Sobelio teigimu, identifikavimo sistemos turi ilgą naudojimo, piktnaudžiavimo socialine kontrole ir diskriminavimo istoriją. Pvz., Sovietų Sąjungoje darbininkų klasei nebuvo išduodami pasai, siekiant apriboti jų judėjimą. Darbininkai, kurie turėjo pasus, galėjo gyventi ir kitose valstybės vietose, bet keliauti galėjo tiktai su milicijos, kuri kontroliavo žmonių judėjimą šalies viduje, leidimu ir tik į tam tikras vietas[205]. JAV Šaltojo karto metu galiojo įstatymas, leidžiantis valstybės sekretoriui savo pasirinkimu asmenims išduoti arba neišduoti paso, atsižvelgiant į viešąjį interesą. Tokia plati diskrecija privedė prie kitų diskriminacinių teisės aktų ir praktikų, tokių kaip, pvz., statutai, neleidžiantys komunistinių organizacijų nariams atnaujinti ar naudotis galiojančiu JAV pasu[206]. Prieš Antrąjį pasaulinį karą nacių Vokietijoje ir karui prasidėjus jos okupuotose teritorijose tapatybės kortelės buvo naudojamos žydams surašyti ir izoliuoti. Kaip pastebi R. Sobelis, visi su žydais susiję Holokausto žiaurumai prasidėjo būtent nuo paprastų surašymų, t. y. nuo jų identifikavimo[207].

Identifikavimas taip pat neleidžia asmeniui išlaikyti anonimiškumo ar pseudonimiškumo. Anonimiškumas ar pseudonimiškumas leidžia žmonėms laisviau balsuoti, kalbėti, burtis į bendruomenes, nes apsaugo nuo išankstinio nusistatymo, šališkumo ar pavojaus, kad su jais bus susidorota. Anonimiškumas gali padidinti ir rašytojo idėjų įtikinamumą, nes skaitytojas, nežinodamas tikslaus autoriaus, gali lengviau priimti jo idėjas, nepaisyti savo išankstinių nusistatymų. Dėl šios priežasties dauguma universitetų egzaminus vertina anonimiškai. Anonimiškumas taip pat suteikia galimybę žmonėms kritikuoti kontroversiškas įmonių, kuriose dirba, praktikas ir be asmeninių pasekmių atskleisti jas kompromituojančių faktų[208]. Negana to, anonimiškumas gali apsaugoti žmones, kurie skaito ar klauso tam tikrų nepopuliarių idėjų[209].

Identifikavimas dažnai yra neatsiejamas kitų privatumo pažeidimų komponentas. Pvz., vienu atveju stebėseną vykdančiam subjektui gali pakakti fiksuoti žmonių skaičių, judėjimą, lytį, apytikrį amžių, bet kitu atveju, kai norima sistemingai stebėti konkretų individą, gali prireikti identifikuoti stebimojo tapatybę. Identifikavimas gali būti agregavimo dalis. Naudojantis agregavimu sukuriamas

---

205 Richard Sobel, „The degradation of political identity under a national identification system“, *BUJ Sci. & Tech. L.* 8 (2002): 52.

206 *Ibid.,* 49.

207 *Ibid.,* 50.

208 Vienas geriausiai žinomų tokių atvejų buvo „Watergate“ skandalas, kuris lėmė JAV prezidento Ričardo Niksono atsistatydinimą, žr. „Watergate Scandal | Summary, Timeline, & Deep Throat“, *Encyclopedia Britannica,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.britannica.com/event/Watergate-Scandal.

209 Solove, „A Taxonomy of Privacy“, *supra note,* 36: 515.

skaitmeninis statistinio žmogaus profilis, susidedantis iš tarpusavyje suderintų fragmentų, o identifikavimas duomenų valdytojui suteikia galimybę žengti dar vieną žingsnį – tą patį skaitmeninio žmogaus profilį tiesiogiai susieti su konkrečiu asmeniu realiame pasaulyje[210].

Naujausios technologijos – pirmiausia tai veido atpažinimo technologijos bei bepiločiai orlaiviai – individų identifikavimo galimybes pakelia į naują lygmenį. Pvz., Kinijos gatvėse jau naudojama paženguси sekimo sistema, kuri automatiškai nustato praeivių tapatybes. Nors Kinijos vyriausybė teigia, kad ši naujovė bus naudojama sekti pabėgėlius ir atrasti dingusius žmones, tačiau ja bus galima ir piktnaudžiauti[211]. Maya Wang[212] teigimu, tokių sistemų tikslas yra suregzti tvirtesnį socialinės kontrolės tinklą, kuris apsunkintų žmonių galimybę planuoti veiksmus prieš vyriausybę arba spausti ją imtis reformų[213]. Vienintelis tokios sistemos apribojimas yra tas, kad stacionarios CCTV kameros, atpažinusios individo veidą, negali jo sekti ten, kur ši stebėjimo sistema neišvystyta. Dar individas gali stebėjimo kamerų sistemingai vengti, tačiau ir šią problemą galima išspręsti – panaudoti bepiločius orlaivius, kuriems ką nors sekti jokių kliūčių nėra.

Bepiločiais orlaiviais surinkti ir į duomenų bazes perkelti vaizdo duomenys, kuriuose individų tapatybės nenustatytos, yra tik skaitmeninės beveidžių žmonių gyvenimo nuotrupos, todėl privatumo pažeidimo tokiu dideliu mastu nėra. Tačiau, jei bepiločiai orlaiviai realiu laiku galėtų atpažinti konkretų stebimąjį, individai galėtų būti susiejami su didelėmis duomenų bazėmis visur ir visada to net nežinodami ir nedavę sutikimo. Nesunku įsivaizduoti scenarijų, kai iš kalinimo įstaigos pabėgus kaliniui valstybės institucija savo paieškos sistemoje įveda šio individo asmens kodą ir paskelbia jo paiešką. Vienu mygtuko paspaudimu pabėgėlio duomenys žaibiškai perduodami milijonams stacionarių vaizdo kamerų, kad šios ieškotų asmens tokiu veidu. Vos tik stacionari kamera atpažįsta pakankamai tikėtiną atitikmenį, sistema automatiškai iš artimiausios stoties paleidžia kameromis ir tokiais pat veido atpažinimo algoritmais apginkluotus bepiločius orlaivius. Po kelių minučių individą iš visų pusių apsupa autonomiškai veikiančių bepiločių orlaivių spiečius, taip akimirksniu identifikuojamas stebimas subjektas ir nustatoma, ar jis kelia pavojų visuomenei. Šie duomenys iškart perduodami operatyviniam policijos būriui, kuris, priklausomai nuo pabėgėlio pavojingumo, imasi atitinkamo lygio sulaikymo veiksmų. Kinijos valdžia atliko eksperimentą, kad parodytų veido atpažinimo technologijos galimybes, ji naudodamasi stacionarių CCTV kamerų sistema su veido atpažinimo algoritmais BBC žurnalistą surado ir sulaikė per

210 *Ibid.,* 514.

211 „In China, Facial Recognition Tech Is Watching You“, *Fortune,* žiūrėta 2019 m. balandžio 9 d., http://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/.

212 Maya Wang yra vyresnioji Kinijos tyrėja JAV įsikūrusioje tarptautinėje nevyriausybinėje organizacijoje „Human Rights Watch“, kurios tikslas stebėti ir ginti žmogaus teises visame pasaulyje.

213 „In China, Facial Recognition Tech Is Watching You“, *supra note,* 215.

7 minutes[214].

Taigi identifikavimo pažeidimas yra susijęs su bepiločiais orlaiviais. Beveik kiekvienas jų turi vaizdo kameras, nesunku įsivaizduoti jas derinamas su veido atpažinimo programine įranga. Būtent identifikavimas sudaro galimybę filmuotoje medžiagoje esantį žmogų susieti su konkrečiu profiliu, o vėliau šią informaciją panaudoti prieš atpažintą asmenį.

1.5.4. Saugumo neužtikrinimas

Duomenys yra vertingas informacijos šaltinis, kuris gali suteikti žinių, o šios – tapti strateginiu pranašumu, įskaitant ir finansinę naudą. Internetinės parduotuvės, analizuodamos savo lankytojų elgseną, gali tiksliau prognozuoti potencialius klientų pirkimo sprendimus. Kai pirkėjo pomėgiai ir įpročiai tampa aiškesni, tikimybė paskatinti jį įsigyti prekes didėja, pavyzdžiui, pasiūlant personalizuotas rekomendacijas, taip sumažinant kliento poreikį aktyviai ieškoti norimų produktų. Individas dažnai nė nepastebi, kaip jo pirkimo istorija, pristatymo duomenys ar palikti atsiliepimai analizuojami ir paverčiami į tikslias įžvalgas apie jo pomėgius, ekonominę padėtį bei potencialius būsimus pirkinius. Tokiu būdu duomenys įgyja ekonominę vertę ir gali būti naudojami komerciniais tikslais. Vienas iš ryškiausių tokios duomenų analizės pritaikymo pavyzdžių – „Amazon“. Pradėjusi veiklą kaip internetinė knygų parduotuvė, ši bendrovė, sistemingai rinkdama ir analizuodama vartotojų elgsenos duomenis, sugebėjo išplėsti savo veiklą ir tapti viena pelningiausių pasaulio kompanijų[215].

Kadangi informacija šiais laikais yra tokia vertinga, tiek ją parduodančių programišių, tiek norinčių ją įsigyti kompanijų juodojoje rinkoje netrūksta, nes kibernetinių atakų skaičius kasmet tiktai auga[216]. Šiuo metu rinkoje būtų sudėtinga rasti didelę internetinės rinkodaros bendrovę, kurios duomenų bazės nebūtų patyrusios kibernetinių įsilaužimų, per kuriuos pavogta milijonų vartotojų asmeninė informacija. Nors jautrūs duomenys, tokie kaip asmeninė elgsenos informacija, slaptažodžiai ar banko kortelių duomenys, turėtų būti kruopščiai saugomi, daugybė didelio masto kibernetinio saugumo incidentų rodo, kad absoliutus duomenų apsaugos užtikrinimas vis dar yra didelis iššūkis. To įrodymas –

214 „China's CCTV Surveillance Network Took Just 7 Minutes to Capture BBC Reporter“, *TechCrunch* (blog), žiūrėta 2019 m. balandžio 29 d., http://social.techcrunch.com/2017/12/13/china-cctv-bbc-reporter/.

215 Harnil Oza, „How Amazon Used Big Data to Rule E-Commerce? | HData Systems“, žiūrėta 2022 m. lapkričio 25 d., https://www.hdatasystems.com/blog/amazon-used-big-data-ai-to-rule-e-commerce.

216 Pvz., vien JAV 2006–2015 m. kibernetinių atakų padaugėjo 1300 proc., žr. „Cyberattacks Against the US Government Up 1,300% Since 2006“, *The Fiscal Times,* žiūrėta 2019 m. balandžio 30 d., http://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006.

„Yahoo“[217] , „Marriott International“[218] ir „Ebay“[219] , įsilaužimai, parodantys, kad net didžiausios pasaulio bendrovės nėra apsaugotos nuo kibernetinių grėsmių.

Daugelis duomenų apsaugos teisės aktų numato, kad asmens duomenys privalo būti tvarkomi tokiu būdu, kad užtikrintų pakankamą saugumo lygį. Pvz., BDAR 5 straipsnio 1 dalies f punktas numato: „Asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas)“[220]. 1974 m. JAV privatumo aktas reikalauja, kad federalinės agentūros, tvarkančios asmens duomenis, įtvirtintų tokias administracines, technines ir fizines apsaugos priemones, kad būtų užtikrintas įrašų saugumas bei konfidencialumas[221]. Vis dėlto vien teisės aktuose įtvirtinta duomenų valdytojų pareiga užtikrinti asmens duomenų saugumą savaime nėra pakankama. Daugybė kibernetinių vagysčių XXI a. rodo, jog duomenis renkantys gigantai yra pajėgesni informaciją kaupti ir analizuoti, negu ją apsaugoti. Duomenų valdytojų negebėjimas apsaugoti sukauptų duomenų vadinamas *saugumo neužtikrinimu*[222].

Bepiločiai orlaiviai su šiuo privatumo pažeidimu gali būti susiję trejopai. Pirma, jie gali rinkti tokią informaciją apie individus, kuri anksčiau buvo neprieinama, todėl bepiločių orlaivių technologija išplečia duomenų, kurie gali būti pavogti iš netinkamai apsaugotų duomenų bazių, apimtį. Pvz., pristatydamas siuntinį į namus bepilotis orlaivis gali užfiksuoti konkretų asmenį, užsisakiusį prekę, nufilmuoti jo namų apylinkes, buitį, taip pat gali užfiksuoti duomenis, kurie sklinda bevieliu ryšiu, kryptiniu mikrofonu pasiklausyti namų gyventojų pokalbių, kitų garsų tuose namuose. Bepiločiai nėra pirma technologija, kuri leidžia kaupti duomenis apie individų elgesį realiame pasaulyje. Kone kiekvienas naudojamės išmaniaisiais telefonais, kurie turi mikrofonus ir filmavimo kameras, kai kurie jau

---

217 2016 m. rugsėjo mėn. „Yahoo“ paskelbė, kad kibernetinės atakos metu iš „Yahoo“ duomenų saugyklų buvo pavogti apie 3 mlrd. vartotojų duomenys, tarp jų tikri vardai, elektroninio pašto adresai, gimimo datos, telefono numeriai, slaptažodžiai, saugumo klausimai; žr. „Yahoo Says 1 Billion User Accounts Were Hacked – The New York Times“, žiūrėta 2020 m. rugpjūčio 27 d., https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

218 2018 m. lapkričio mėn. „Marriott International“ paskelbė, kad kibernetiniai vagys pavogė apie 500 mln. vartotojų duomenis. Pasak „The New York Times“, už ataką buvo atsakinga Kinijos žvalgyba; žr. David E. Sanger ir kt., „Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing“, *The New York Times,* 2018 m. gruodžio 11 d., https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

219 Prekybos internetu gigantas „Ebay“ 2014 m. paskelbė, kad per kibernetinę ataką buvo pavogti 145 mln. vartotojų duomenys; žr. „eBay asks 145 million users to change passwords after data breach – The Washington Post“, žiūrėta 2020 m. rugpjūčio 27 d., https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/.

220 BDAR.

221 The Privacy Act of 1974, pakeistas 5 U.S.C. § 552a.

222 „A Taxonomy of Privacy“, *supra note,* 36: 516–522.

naudojasi išmaniaisiais namų asistentais, tokiais kaip „Amazon Echo Dot“ ar „Google Home“, kurie turi galingus mikrofonus. Teoriškai labai daug informacijos apie žmogaus elgesį realiame gyvenime galima kaupti pasitelkiant vien šiuos įrenginius. Tačiau bepiločiai orlaiviai, kaip ir minėtos technologijos, prie saugumo neužtikrinimo prisideda, nes padeda didelę galią rinkoje turintiems subjektams dar vienu būdu rinkti duomenis apie asmenų elgesio struktūras, o galiausiai sukaupę didžiulės apimties duomenis negali jų apsaugoti nuo kibernetinių atakų.

Antra, kibernetiniai užpuolikai gali įsilaužti ne tik į duomenų bazes, kuriose kaupiami bepiločiais orlaiviais surinkti duomenys, bet ir į patį bepilotį orlaivį, kurio veikimas visiškai priklauso nuo bevielio duomenų ryšio, susiejančio skirtingus jo komponentus. Kiekvienas bepilotis orlaivis turi skirtingas ryšių sąsajas, kurioms apsaugoti yra naudojamos skirtingos apsaugos priemonės, pvz., skraidomoji bepiločio orlaivio dalis beveik visais atvejais bevieliu 4G ar belaidžiu ryšiu būna susieta su valdymo stotimi, taip pat GPS ar „Galileo“ ryšiu su palydovu žemės atmosferoje. Autonominiai bepiločiai orlaiviai gali papildomai būti susieti tarpusavyje, kad sudarytų kolektyvinį spiečių. Mokslinėje literatūroje rašoma, kad palydovinį ir tiesioginį duomenų ryšį (kai bepilotis valdomas tiesiogiai iš neprijungtos prie interneto valdymo stoties) perimti sudėtingiau, nes šiems ryšiams apsaugoti egzistuoja gana patikimos apsaugos priemonės[223], o į belaidžius tinklus įsibrauti įmanoma gana lengvai, nes jiems apsaugoti naudojami metodai yra nesaugūs ir nepatikimi[224]. Įsiveržę į individualų bepilotį orlaivį programišiai gali perimti jo valdymą, slapta stebėti ir pasiklausyti aplinkos per jo vaizdo kameras bei mikrofonus, nustatyti asmenų buvimo vietą[225]. Nors įsilaužimas į atsitiktinio individualaus bepiločio sistemą gali atrodyti savaime nelabai pavojingas, kadangi, galima manyti, pažeidžiamas tiktai orlaivio valdytojo privatumas, bet problema slypi giliau. Įsilaužimas į bepilotį orlaivį tinkamoje vietoje ir tinkamu laiku gali sukelti grėsmę daugelio kitų žmonių privatumui, nes perimtas bepilotis orlaivis gali būti panaudojamas piktadarystėms ne tik prieš jo valdytoją bet ir prieš kitus individus.

Iš to kyla trečiasis saugumo neužtikrinimo aspektas – patys bepiločiai orlaiviai gali būti priemonės kibernetiniams išpuoliams vykdyti. Pvz., bepiločiai orlaiviai gali būti naudojami nusikaltimo vietoms modifikuoti. Pasitelkę juos nusikaltėliai galėtų iš įvykio vietos pašalinti savo nusikaltimo pėdsakus arba pridėti padirbtų pėdsakų ir tokiu būdu sudaryti pagrindą klaidingiems kaltinimams. Pirštų antspaudus jau ir dabar įmanoma padirbti specialiu spausdintuvu, šią technologiją tiesiog reikėtų pritaikyti bepiločiams orlaiviams[226]. Dar vienas pavyzdys

---

223 Ahmad Javaid ir kt., „Cyber security threat analysis and modeling of an unmanned aerial vehicle system“, 2012, p. 586, https://doi.org/10.1109/THS.2012.6459914.

224 Theodore Reed, Joseph Geis ir Sven Dietrich, „SkyNET: A 3G-Enabled Mobile Attack Drone and Stealth Botmaster“, *WOOT,* 2011, 28–36.

225 Fred Samland ir kt., „AR.Drone: Security threat analysis and exemplary attack to track persons“, *Proceedings of SPIE – The International Society for Optical Engineering* 8301 (2012 m. sausio 22 d.): 15, https://doi.org/10.1117/12.902990.

226 *Ibid.*

galėtų būti naujos kartos *botų* tinklai. Mokslininkų grupė neseniai pristatė bepilotį orlaivį, kuriuo galima automatiškai aptikti ir įsilaužti į belaidžius tinklus. Savo straipsnyje Theodore'as Reedas, Joseph'as Geisas ir Svenas Dietrichas pristato plačiai naudojamą įsilaužimo į vietinius belaidžius tinklus sistemą – *botų tinklą*[227], kuri, pasak autorių, šiuo metu yra didžiausia grėsmė kibernetiniam saugumui, ir pateikia savo tinklo variantą – „SkyNET", kuriuo galima įsilaužti į asmenų kompiuterius ne per internetą, o pasitelkus bepilotį orlaivį nulaužti vietinius belaidžius tinklus. Įprastą *botų tinklą* internetu kontroliuoja *botmasteris*[228], tačiau tokiu būdu veikiantys botų tinklai pasitelkiant šiuolaikines kibernetinio saugumo priemones jau gali būti susekami, o per „SkyNET" bepiločiai orlaiviai gali būti kontroliuojami be interneto pagalbos, todėl apeina tokias tradicines interneto tinklų apsaugos priemones kaip ugniasienės (angl. *firewalls*), įsilaužimo aptikimo sistemos (angl. *intrusion detection systems*) ir įvykių registravimas (angl. *event logging*). Negana to, asmeninių belaidžių tinklų apsauga paprastai būna labai silpna, todėl per juos įsilaužti į šeimininko kompiuterį visai nesudėtinga[229]. Taigi „SkyNET" padeda programišiams lengvai įsilaužti į žmonių asmeninius kompiuterius tiesiog bepiločiu orlaiviu praskrendant pro juos dominančią vietovę[230], belieka tik įsivaizduoti, kokio masto kibernetiniai nusikaltimai galėtų būti įvykdyti, jeigu į darbą būtų paleistas ne vienas, o šimtai ar tūkstančiai „SkyNET" principu veikiančių bepiločių orlaivių. Kaip matyti iš atliktos analizės, bepiločiai orlaiviai prie privatumo pažeidimo, neužtikrindami saugumo, prisideda labai reikšmingai ne tik dėl to, kad didina surinktos informacijos kiekį nesaugiose duomenų bazėse, bet ir dėl to, kad patys įgalina programišius vykdyti kibernetinius nusikaltimus, kurie dar visai neseniai buvo tik mokslinės fantastikos sritis.

1.5.5. Atidengimas

Atidengimas yra privatumo pažeidimo forma, kai tretiesiems asmenims atskleidžiamos tam tikros individo fizinės savybės ar emocinės būsenos, kurios gali sukelti diskomfortą, pažeminimo jausmą ar stigmatizaciją. Toks informacijos atskleidimas gali apimti įvairius asmeninius ir jautrius aspektus, tokius kaip sielvartas, kančia, trauma, sužeidimai, nuogumas, lytiniai santykiai ar fiziologiniai procesai. Nepaisant to, kad šie reiškiniai yra neatsiejama žmogaus egzistencijos dalis,

---

227 Terminas *botnet* į lietuvių kalbą galėtų būti verčiamas kaip *botų tinklas,* o terminas *botas* pagal „Cambridge Dictionary" suprantamas kaip „kompiuterinė programa, kuri veikia autonomiškai, ypač ta, kuri ieško ir randa informaciją internete: nusikaltėliai sukuria botų tinklus, kurie klajoja internete užkrėsdami asmeninius kompiuterius kenkėjiškomis programomis" (vertė D. K.). „BOT | Meaning in the Cambridge English Dictionary", žiūrėta 2019 m. gegužės 7 d., https://dictionary.cambridge.org/dictionary/english/bot.

228 Terminas *botmaster* į lietuvių kalbą galėtų būti verčiamas kaip *botmasteris*. Šis terminas reiškia asmenį arba programą, kuri kontroliuoja botų tinkle esančius pavienius botus.

229 Reed, Geis and Dietrich, *supra note,* 228: 1–2.

230 *Ibid.,* 3.

socialinės normos ir kultūriniai kontekstai dažnai lemia jų suvokimą kaip privačių ir potencialiai žeminančių. Šiuolaikinėje visuomenėje tokie procesai dažnai siejami su individo pažeidžiamumu ir silpnumu, o tam tikros veiklos gali būti laikomos socialiai nepriimtinomis ar net stigmatizuojamomis. Dėl to daugelis asmenų siekia apsaugoti šią informaciją nuo viešo atskleidimo, laikydami ją esmine savo privatumo dalimi[231].

Suvokimas apie kūno viešą demonstravimą ir jo funkcijas skirtingais istorijos laikotarpiais kito priklausomai nuo kultūrinių ir socialinių normų[232]. Viduramžiais kolektyvinis maudymasis, įskaitant nuogumą nepažįstamųjų akivaizdoje, buvo įprastas reiškinys ir nesukeldavo socialinio diskomforto, nes kūnas nebuvo suvokiamas kaip privati sfera, reikalaujanti ypatingos apsaugos. Tačiau nuo XVI a. Europoje pradėjo formuotis nuostata, jog kūnas turėtų būti slepiamas, o nuogumas vis dažniau buvo siejamas su gėda ar nepadorumu. Antikinėje Graikijoje nuogumas buvo laikomas ne tik socialiai priimtinu, bet ir simbolizavo fizinę bei moralinę stiprybę. Tuo tarpu Renesanso laikotarpiu aukštuomenėje įsitvirtino didesnio kuklumo ir savidisciplinos principai, o kūno bei jo funkcijų viešas demonstravimas imtas laikyti netinkamu elgesiu[233]. Šiuolaikinės socialinės normos išlaiko šią tradiciją, nustatydamos aiškias ribas tarp to, kas laikoma viešu ir privačiu. Dėl šios priežasties kūno ar jo funkcijų atidengimas be asmens sutikimo dažnai vertinamas ne tik kaip privatumo, bet ir kaip žmogaus orumo pažeidimas. Kaip teigia D. J. Solove'as, orumas, suvokiamas šiuolaikiškai, leidžia individui įveikti savo instinktyvią prigimtį ir tapti civilizuotu[234].

Daugeliu atvejų asmens nuogumas, lytiniai santykiai ar fiziologinių poreikių tenkinimas nėra vertinami kaip jo socialinio statuso ar civilizuotumo rodiklis. Vis dėlto, kai tokio pobūdžio privatūs momentai be individo sutikimo atskleidžiami tretiesiems asmenims, tai gali sukelti stiprų psichologinį diskomfortą, pažeidžiamumo jausmą ir menkavertiškumo išgyvenimus. Net ir pats žinojimas, kad apie asmenį buvo surinkta ar saugoma tokia informacija, gali skatinti nesaugumo jausmą, nerimą ar net paranoją. Jei ši informacija tampa viešai prieinama, individas gali patirti socialinį pažeminimą, kuris gali reikšmingai paveikti jo savivertę ir pasitikėjimą savimi. Nors visuomenė paprastai neteisia tokios informacijos atskleidimo aukų, kadangi aptariama informacija nėra konceptualiai nauja ar nesuprantama, pats privatumo pažeidimas gali turėti reikšmingų neigiamų psichologinių pasekmių nukentėjusiajam[235].

Bepiločiai orlaiviai reikšmingai prisideda prie privatumo pažeidimų, nes jų technologinės galimybės leidžia lengvai fiksuoti asmenis privačioje erdvėje, jiems atliekant asmeninio pobūdžio veiklas. Šiuolaikinės stebėjimo technologijos suteikia precedento neturinčias galimybes vykdyti vojeristinę

231 Solove, „A Taxonomy of Privacy", *supra note,* 36: 536.
232 *Ibid.,* 537.
233 Solove, „Conceptualizing privacy", *supra note,* 36: 1087–1156.
234 Solove, „A Taxonomy of Privacy", *supra note,* 36: 537.
235 *Ibid.,* 538.

veiklą, o bepiločiais orlaiviais užfiksuotų tokių atvejų vis daugėja[236]. Nors kompromituojanti vaizdo medžiaga dažniausiai nėra viešai paviešinama, pats suvokimas, kad asmuo gali būti stebimas per namų langus, sukelia nuolatinį psichologinį diskomfortą ir gali būti traktuojamas kaip privatumo pažeidimas. Individas, suvokdamas, kad net ir būdamas visiškai vienas savo namuose nėra apsaugotas nuo galimo stebėjimo, gali patirti nuolatinę įtampą, nesaugumo jausmą bei kitas neigiamas emocines reakcijas. Psichologiniai išgyvenimai tampa dar intensyvesni, jei užfiksuota vaizdo medžiaga tampa viešai prieinama. Tokie atvejai dažniausiai pasitaiko viešiems asmenims[237], tačiau nėra atmetama galimybė, kad kompromituojanti informacija gali būti panaudota ir šantažo tikslais[238], taip dar labiau didinant nukentėjusiojo pažeidžiamumą.

Prieš kelis dešimtmečius dauguma asmenų, būdami savo namų aplinkoje, net nesvarstydavo galimybės, kad gali būti stebimi per langus ar uždarame kieme. Tačiau bepiločių orlaivių atsiradimas iš esmės pakeitė šią situaciją. Šiuo metu šių orlaivių prieinamumas sparčiai didėja, todėl net ir tie, kurie gyvena dangoraižiuose ar turi privačius, aptvertus kiemus, negali būti visiškai tikri, jog jų privatumas nėra pažeidžiamas bepiločio orlaivio stebėjimo priemonėmis. Nors pats bepilotis orlaivis tėra technologinis įrankis, naudojamas informacijos rinkimui, jo vaidmuo atidengimo pažeidimo kontekste yra reikšmingas. Be tokių priemonių asmeninių

---

236 Žr. Chris Matyszczyk, „Man Shoots down Drone Hovering over House“, CNET, žiūrėta 2019 m. gegužės 13 d., https://www.cnet.com/news/man-shoots-down-drone-hovering-over-house/. (JAV vyras šautuvu numušė virš savo žemės sklypo pakibusį bepilotį orlaivį neva dėl to, kad buvo stebima kieme besideginanti šešiolikmetė dukra.); *Nordwest-Zeitung,* „Albtraum In Bremen: Drohne schaut ins“, 2018 m. liepos 30 d., https://www.nwzonline.de/bremen/bremen-albtraum-in-bremen-wenn-eine-drohne-ins_a_50,2,481666789.html. (Pora iš Bremeno policijai pateikė pranešimą apie pro miegamojo langą juos stebintį bepilotį orlaivį.); Von Sabine Norgall, „Drohne spionierte durchs Fenster“, *Mittelbayerische Zeitung,* žiūrėta 2019 m. gegužės 13 d., https://www.mittelbayerische.de/region/regensburg-land-nachrichten/drohne-spionierte-durchs-fenster-21364-art1741147.html. (Kita pora iš Regestauf, Vokietijos, taip pat policijai teigė, kad kažkas dronu juos stebėjo per svetainės langus.); Sophia Choi, „Atlanta Woman Says Drone ‘peeped’ on Her While She Dressed“, WSBTV, 2018 m. gegužės 15 d., https://www.wsbtv.com/news/local/atlanta-woman-says-drone-peeped-on-her-while-she-dressed/747083812. (Moteris iš Atlantos, JAV, skundėsi, jog per dangoraižyje esančio buto langus dronu kažkas stebėjo, kaip ji rengiasi.)

237 „Hollywood celebrities besieged by drones – and you could be next“, *Mail Online,* 2014 m. rugsėjo 6 d., https://www.dailymail.co.uk/news/article-2746231/Attack-drones-Hollywood-celebrities-besieged-paparazzi-spies-sky-Worried-You-ll-soon-regular-fixture-YOUR-home.html.

238 Pvz., vieną šantažo atvejų puikiai perteikia mokslinės fantastikos serialo „Juodasis veidrodis“ (angl. *Black Mirror*) serija „Užsičiaupk ir šok“ (angl. *Shut Up and Dance*), kurioje pagrindinio veikėjo, devyniolikmečio, kompiuteris užkrečiamas virusu. Jam nežinant kenkėjiška programa aktyvuoja nešiojamojo kompiuterio vaizdo kamerą, kuri užfiksuoja kaip devyniolikmetis lytiškai save tenkina žiūrėdamas pornografiją. Įsilaužėliai vėliau grasina paviešinti vaizdo įrašą, jeigu serialo veikėjas nevykdys jų įsakymų; žr. James Watkins, *Shut Up and Dance, Drama, Sci-Fi, Thriller* (*House of Tomorrow,* 2016).

erdvių stebėjimas būtų daug sudėtingesnis arba apskritai neįmanomas, todėl bepiločių orlaivių naudojimas tampa esmine sąlyga, leidžiančia vykdyti privatumo pažeidimus dažniau ir efektyviau.

1.6. Skyriaus išvados. Kuo bepiločiai orlaiviai skiriasi nuo kitų privatumą galinčių pažeisti technologijų?

Per privatumo pažeidimų prizmę atlikta analizė parodė, kad bepiločiai orlaiviai yra rimta grėsmė privatumui. Šiame disertacijos skyriuje aptarti būdai, kuriais privatumą buvo įmanoma pažeisti ir anksčiau, tačiau pradėjus naudoti bepiločius orlaivius privatumo pažeidimų dažnumas ir sunkumas gali gerokai išaugti. Atlikus analizę nustatytos kelios pagrindinės priežastys, dėl kurių bepiločiai orlaiviai gali būti posūkio tašku, lemsiančiu privatumo koncepcijos pokyčius.

Ribų tarp virtualaus ir realaus pasaulio nykimas. Bepiločiai orlaiviai iš esmės transformuoja stebėjimo pobūdį, panaikindami ribas tarp virtualaus ir realaus pasaulio. Tradiciškai stebėsena virtualioje erdvėje, vykdoma per išmaniuosius įrenginius, socialinius tinklus ir interneto paslaugas, buvo labiau ribota ir prognozuojama. Tačiau naudojant bepiločius orlaivius, stebėjimas realiame pasaulyje tampa daug agresyvesnis ir invazyvesnis. Jie gali rinkti informaciją apie asmenų buvimo vietą, elgesį ir veiksmus realiu laiku, darydami tai nepastebimai ir iš įvairių kampų. Kai šie duomenys yra sujungiami su informacija, surinkta virtualioje erdvėje per išmaniuosius įrenginius, tai gali padaryti neigiamą poveikį privatumui. Toks informacijos agregavimas iš abiejų šaltinių gali sukurti išsamų ir detalų asmens elgesio, pomėgių ir kasdienybės profilį. Tai ne tik kelia didelę grėsmę privatumui, bet ir suteikia valstybinėms ir privačioms institucijoms precedento neturinčias galimybes individais manipuliuoti ir juos kontroliuoti.

Platus naudojimo mastas. Lanksčios bepiločių orlaivių pritaikymo galimybės, taip pat maža kaina, nedideli gabaritai lems tai, jog netolimoje ateityje danguje jų bus labai daug. Danguje vis daugėjant asmens duomenis galinčių fiksuoti robotų skaičiui atsiranda dar daugiau galimybių galingiems informacijos infrastruktūrą valdantiems viešiems bei privatiems subjektams užfiksuotą informaciją panaudoti savo tikslams pasiekti.

Stebėjimo intensyvumas. Bepiločiais orlaiviais žmones įmanoma stebėti nuolatos ir iš labai arti, o užfiksuotus vaizdus dėti į laikmenas, kur jie vėliau gali būti iš naujo atrasti ir perdirbti. Iki atsirandant bepiločiams orlaiviams, intensyviausio stebėjimo sistema buvo CCTV stebėjimo kameros, kurios pritaisytos prie stacionarių objektų, dėl to jų patikimumas detaliai atkurti įvykius ar žmones ribotas.

Stebėjimo kampų įvairovė. Bepiločiai orlaiviai gali įveikti kliūtis, esančias jų matymo linijoje ir dėl skraidymo galimybių fiksuoti tokius vaizdus, kurių prie nejudančio objekto pritaisyta kamera negalėtų užfiksuoti. Naudojant specialią programinę įrangą bepiločiu orlaiviu ar jų spiečiumi galima užfiksuoti netgi trimatį stebimo objekto vaizdą, ko negalėtų pasiūlyti iki bepiločių orlaivių naudotos stebėjimo priemonės. Nuolatinę stebėseną bepiločiais orlaiviais galima vykdyti

ne tik viešose vietose, kur ir taip daug stacionarių stebėjimo kamerų, bet ir, pvz., prie stebimojo durų slenksčio.

Galimybė tapti ginklu. Bepiločiai orlaiviai gali būti apginkluoti ir kamera, ir siųstuvais, kurie gali padėti atlikti kibernetinę ataką, ir garsiakalbiais, kuriais gali būti bandoma įbauginti taikų asmenų susibūrimą, ir netgi tikrais ginklais, kuriais galima pasikėsinti į asmens gyvybę ar jo turtą. Ši išskirtinė bepiločių orlaivių savybė leidžia jų valdytojams ne tik pasyviai stebėti, bet ir užfiksavus nepageidaujamą elgesį nedelsiant veikti, o tai dar labiau sustiprina jų sukeliamą atšalimo efektą visuomenėje. Bepiločius orlaivius paversti skraidančiais ir visa matančiais ginklais, kuriais be reikšmingų apribojimų naudojasi valstybės apsaugos tarnybos, užtektų neapgalvoto valdžios institucijų sprendimo, pvz., kilus krizei. Tad šiuo požiūriu bepiločiai orlaiviai pavojingiausi – biurokratų rankose.

Nepastebimumas. Bepiločiai orlaiviai gali būti įvairių konfigūracijų. Kai kurie būna dideli ir skleidžia daug garso, juos lengva pastebėti. Vis dėlto tikėtina, jog stebėsenai pritaikyti bepiločiai orlaiviai įgis įvairių „nematomų" formų, pvz., Kinija jau dabar kuria bepiločius orlaivius, kurie panašūs į balandžius. Ateityje sekti naudojami bepiločiai orlaiviai tikriausiai primins vos įžiūrimus vabzdžius. Tokių bepiločių orlaivių stebimi individai nežinos: nei kokiu pagrindu yra sekami, nei kad apskritai yra sekami, nei kokius su jais susijusius sprendimus priims duomenis kaupiantys subjektai, kurie naudosis surinkta informacija.

Paminėtoms priežastims reikėtų suteikti daugiau konteksto. Paprasčiausias būdas tai padaryti būtų palyginti, ar bepiločiai orlaiviai tikrai išsiskiria iš jau naudojamų kitų technologijų, gebančių pažeisti privatumą. Palyginimui pasirinktos šios technologijos: išmanieji telefonai, CCTV kameros, socialinių tinklų platformos (pvz. Facebook, Instagram, LinkedIn), išmanieji namų asistentai (pvz., Amazon Echo, Google Home) bei slapukai internete (cookies). Kiekviena iš jų aptariama atskirai per identifikuotų priežasčių prizmę.

Išmanieji telefonai renka daug informacijos apie naudotojų veiklą, įskaitant buvimo vietą, naršymo istoriją, programėlių naudojimą ir asmeninius ryšius. Tačiau šie duomenys yra riboti telefono savininko kontekste ir dažniausiai lieka virtualioje erdvėje. Priešingai, bepiločiai orlaiviai gali stebėti žmones realiame pasaulyje be jų žinios, fiksuodami jų buvimo vietą, elgesį ir veiksmus realiu laiku. Kai bepiločių orlaivių surinkti duomenys sujungiami su išmaniojo telefono duomenimis, ribos tarp virtualaus ir realaus pasaulio nyksta, sukuriant išsamų ir detalų asmens profilį, ko negali atlikti vien tik išmanieji telefonai. Platus bepiločių orlaivių naudojimo mastas, lanksčios pritaikymo galimybės, maža kaina ir nedideli gabaritai išmaniems telefonams būdingos savybės, kaip ir bepiločiams orlaiviams. Tačiau platus išmaniųjų telefonų naudojimas nelemia tokio išsamaus realaus pasaulio stebėjimo kaip bepiločių orlaivių naudojimas. Negana to, išmanieji telefonai veikia tik ten, kur yra ryšys. Tuo tarpu bepiločiai orlaiviai galėtų veikti nepriklausomai nuo interneto prieigos. Stebėjimo intensyvumas taip pat skiria bepiločius orlaivius nuo išmaniųjų telefonų. Išmanieji renka duomenis tik tada, kai yra naudojami, o bepiločiai orlaiviai gali nuolat stebėti žmones iš arti ir realiame pasaulyje, įrašydami

detalius vaizdus ir garsus, kurie gali būti perdirbti vėliau. Tai leidžia bepiločiais fiksuoti daug daugiau informacijos apie žmonių kasdienį gyvenimą nei išmaniaisiais telefonais. Stebėjimo kampų įvairovė yra dar vienas aspektas, kuriuo bepiločiai stebėjimo aspektu pranašesni už išmaniuosius telefonus. Bepiločiai orlaiviai gali įveikti kliūtis, skraidydami įvairiomis kryptimis ir fiksuodami vaizdus iš skirtingų kampų bei aukščių, kas leidžia surinkti daug išsamesnius realaus pasaulio vaizdo duomenis nei tie, kurie surenkami išmaniaisiais telefonais. Išmaniųjų telefonų vaizdo duomenų detalumas priklauso nuo lauko, kurį apima prie telefono pritaisyta kamera. Bepiločius taip pat galima naudoti kaip ginklus, tuo tarpu išmanieji telefonai įprasti negali būti tiesiogiai naudojami fiziniam poveikiui. Galiausiai, nepastebimumas yra dar vienas aspektas, kuriuo bepiločiai orlaiviai išsiskiria nuo išmaniųjų telefonų. Išmanieji telefonai yra lengvai pastebimi ir dažniausiai priklauso konkrečiam asmeniui, kuris žino apie jų buvimą. Bepiločiai orlaiviai gali būti mažo dydžio, suprojektuoti taip, kad būtų nepastebimi ir galėtų stebėti žmones realiame pasaulyje be jų žinios. Toks slapta atliekamas stebėjimas derinamas su kitomis privatumą galinčiomis pažeisti technologijomis suteikia precedento neturinčias galimybes manipuliuoti ir kontroliuoti asmenis, ko negalima pasiekti vien išmaniaisiais telefonais.

CCTV kameros[239] taip pat renka daug informacijos apie žmonių veiklą, fiksuodamos vaizdus viešose ir privačiose vietose, šiuo aspektu jos prisideda prie ribų tarp virtualaus ir realaus pasaulio nykimo. Tačiau jų stebėjimas yra labiau ribotas ir prognozuojamas, nes kameros yra stacionarios ir veikia tik tam tikroje vietoje. Bepiločiai orlaiviai, priešingai, dėl savo mobilumo ir gebėjimo skraidyti įvairiomis kryptimis, gali rinkti vaizdo duomenis daug platesniu mastu. Jie gali fiksuoti asmenų buvimo vietą, elgesį ir veiksmus realiu laiku, nepastebimai ir iš įvairių kampų, kas sukuria išsamesnį asmens profilį nei vien vaizdo duomenų rinkimas CCTV kameromis. CCTV kameros taip pat kaip ir bepiločiai orlaiviai pasižymi lankčiais pritaikymo būdais, maža kaina ir nedideliais gabaritais, tačiau bepiločių mobilumas leidžia jiems veikti įvairiose aplinkose, kur CCTV kameros praktiškai nepritaikomos. Plačiai naudojamos CCTV kameros nesuteikia tokio išsamaus realaus pasaulio stebėjimo kaip bepiločių orlaivių technologijos. Stebėjimo intensyvumas taip pat skiria bepiločius orlaivius nuo CCTV kamerų. CCTV kameros fiksuoja vaizdus tik savo aprėpties zonoje ir dažniausiai yra stacionarios, o bepiločiai orlaiviai gali nuolat sekti žmones iš arti realiame pasaulyje, įrašydami detalius vaizdus ir garsus, kurie gali būti analizuojami vėliau. Tai leidžia bepiločiais surinkti daug daugiau informacijos apie žmonių kasdienį gyvenimą nei CCTV kameromis. Stebėjimo kampų įvairovė yra dar vienas aspektas, kuriuo bepiločiai orlaiviai pranašesni už CCTV kameras. Bepiločiai orlaiviai gali įveikti kliūtis, skraidydami

239 Vertėtų patikslinti, kad analizei pasirenkamos būtent stacionarios, dažniausiai prie pastatų pritvirtinamos filmavimo kameros. Lyginti bepiločius su bet kokiomis filmavimo kameromis nebūtų logiška, nes būtent filmavimo kameros ir yra vienas iš bepiločių orlaivių komponentų, dėl kurių bepiločiai orlaiviai kelia grėsmę privatumui.

įvairiomis kryptimis ir fiksuodami vaizdus iš skirtingų kampų bei aukščių, kas leidžia surinkti daug išsamesnius vaizdo duomenis nei tie, kurie surenkami CCTV kameromis. CCTV kamerų vaizdo duomenų detalumas priklauso nuo kampo ir vietos, kur jos yra sumontuotos. Bepiločiai orlaiviai taip pat gali būti panaudoti kaip ginklai, tuo tarpu fizinis poveikis žmonėms CCTV kameromis, nors ir įmanoma, tačiau stipriai ribojamas dėl CCTV kamerų stacionarumo. Galiausiai, nepastebimumas yra dar vienas aspektas, kuriuo bepiločiai orlaiviai išsiskiria nuo CCTV kamerų. CCTV kameros dažniausiai yra lengvai pastebimos ir montuojamos aiškiai matomose vietose. Bepiločiai orlaiviai gali būti mažo dydžio ir suprojektuoti taip, kad būtų beveik nematomi, leidžiant jiems slapta stebėti žmones realiame pasaulyje be jų žinios.

Socialinių tinklų platformos renka daug informacijos apie vartotojų veiklą, įskaitant jų pomėgius, ryšius ir elgesį internete. Tačiau šie duomenys dažniausiai lieka virtualioje erdvėje ir yra riboti naudotojų pateiktais duomenimis bei jų veikla platformose. Priešingai, bepiločiai orlaiviai gali stebėti žmones realiame pasaulyje be jų žinios, fiksuodami jų buvimo vietą, elgesį ir veiksmus realiu laiku. Kai bepiločių orlaivių surinkti duomenys sujungiami su socialinių tinklų platformose sukaupta informacija, ribos tarp virtualaus ir realaus pasaulio nyksta, sukuriant išsamų ir detalų asmens profilį, ko negalima atlikti vien pasitelkiant socialinių tinklų platformas. Socialinių tinklų platformos plačiai naudojamos visame pasaulyje ir turi milijonus vartotojų, tačiau jų naudojimas yra ribotas virtualia erdve. Tuo tarpu bepiločiai orlaiviai dėl savo mobilumo, lanksčių pritaikymo galimybių, mažos kainos ir nedidelių gabaritų, gali veikti daugelyje skirtingų aplinkų realiame pasaulyje. Jie gali rinkti informaciją didesniu mastu ir įvairiose vietose, kur socialinių tinklų platformos neįmanomos naudoti. Bepiločiai orlaiviai taip pat gali veikti nepriklausomai nuo interneto prieigos, priešingai nei socialinių tinklų platformos. Stebėjimo intensyvumas taip pat skiria bepiločius orlaivius nuo socialinių tinklų platformų. Socialinių tinklų platformos gali stebėti ir analizuoti naudotojų veiklą tik virtualioje erdvėje, o jų galimybės apribotos naudotojų pateiktais duomenimis. Bepiločiai orlaiviai gali skraidyti įvairiomis kryptimis ir fiksuoti vaizdus iš skirtingų kampų bei aukščių, kas leidžia surinkti išsamesnius vaizdo duomenis nei naudojantis duomenimis įkeliamais į socialinių tinklų platformas. Stebėjimo intensyvumas taip pat skiria bepiločius orlaivius nuo socialinių tinklų platformų. Socialinių tinklų duomenys yra riboti naudotojo veikla platformoje, o bepiločiai gali nuolat stebėti žmones iš arti ir realiame pasaulyje, įrašydami detalius vaizdus ir garsus, kurie gali būti perdirbti vėliau, ir derinami su virtualioje erdvėje surinkta informacija. Stebėjimo kampų įvairovė yra dar vienas aspektas, kuriuo bepiločiai įkyresni už socialinių tinklų platformas. Bepiločiai orlaiviai gali įveikti kliūtis, skraidydami įvairiomis kryptimis ir fiksuodami vaizdus iš skirtingų kampų bei aukščių, kas suteikia daug išsamesnį stebėjimo vaizdą nei statiniai socialinių tinklų duomenys. Bepiločiai orlaiviai taip pat gali būti panaudoti kaip fiziniai ginklai, siekiant realioje erdvėje įbauginti žmones, tuo tarpu žmones per socialinius tinklus paveikti įmanoma nebent psichologiškai. Galiausiai, nepastebimumas yra dar

vienas aspektas, kuriuo bepiločiai orlaiviai skiriasi nuo socialinių tinklų platformų. Viena vertus, socialiniai tinklai gali veikti nepastebimai net ir su vartotojo sutikimu, pavyzdžiui, jei vartotojas mechaniškai sutinka su socialinio tinklo privatumo politika jos neperskaitęs, ir vėliau socialinis tinklas vartotoją „šnipinėja“ per išmaniojo telefono mikrofoną, kad pateiktų vartotojo poreikius labiau atitinkantį reklamų turinį. Tokiu pasiklausymu socialiniai tinklai įsiveržia į realią žmogaus privačią erdvę, panašiai kaip ir bepiločiai orlaiviai. Tačiau šnipinėjimas bepiločiais orlaiviais, kurie būtų vabzdžio dydžio, galėtų būti kur kas intensyvesnis ir išsamesnis nei socialinių tinklų. Bepiločiais taip pat galima būtų fiksuoti ne tik garso, bet ir vaizdo duomenis iš įvairių kampų.

Išmanieji namų asistentai renka daug informacijos apie individų veiklą namuose, įskaitant balso komandas, įrenginių naudojimą, aplinkos garsus, kurie dažniausiai siunčiami į išmaniųjų namų asistentais prekiaujančių įmonių serverius. Juose duomenys toliau gali būti išsaugomi ir agreguojami. Tačiau šie duomenys dažniausiai riboti namų aplinka. Priešingai nei išmanieji namų asistentai, bepiločiai orlaiviai gali judėti laisvai ir stebėti žmones tiek namuose, tiek viešose vietose, kas suteikia platesnį stebėjimo spektrą ir leidžia sujungti duomenis iš skirtingų šaltinių. Šiuo aspektu bepiločiai labiau prisideda prie ribų tarp virtualaus ir realaus pasaulio nykimo. Platus bepiločių orlaivių naudojimo mastas yra dar vienas svarbus aspektas. Išmanieji namų asistentai plačiai naudojami namuose, tačiau tolesnis jų pritaikymo galimybių vystymasis yra ribotas dėl jų fiksuotos vietos namų aplinkoje. Stebėjimo intensyvumas taip pat skiria bepiločius orlaivius nuo išmaniųjų namų asistentų. Bepiločiai orlaiviai gali nuolat stebėti žmones realiame pasaulyje, įrašydami detalius vaizdus ir garsus, kurie gali būti analizuojami vėliau. Išmanieji namų asistentai renka duomenis tik tada, kai yra aktyvuojami vartotojų ir tik tose vietose, kur jie yra įrengti, todėl jų stebėjimo intensyvumas yra ribotas. Stebėjimo kampų įvairovė yra dar vienas aspektas, kuriuo bepiločiai orlaiviai invazyvesni už išmaniuosius namų asistentus. Bepiločiai orlaiviai gali skraidyti įvairiomis kryptimis ir fiksuoti vaizdus iš skirtingų kampų bei aukščių, kas suteikia daug išsamesnius stebėjimo duomenis. Tuo tarpu stacionarūs namų asistentai renka informaciją tik iš fiksuotos vietos, todėl jų stebėjimo kampas yra ribotas. Tiesa, siekiant užtikrinti namų apsaugą, stacionarūs namų asistentai gali būti susiejami ir su kitais stebėjimo įrenginiais tokiais kaip CCTV kameros, įvairūs jutikliai, net ir bepiločiai orlaiviai, kas išplėstų jų galimybes individus stebėti iš įvairių kampų. Be to, bepiločiai orlaiviai turi galimybę tapti ginklu, kas yra išskirtinė jų savybė. Prie bepiločių gali būti pritaisyti tikri ginklai, kas leidžia jiems ne tik pasyviai stebėti, bet ir aktyviai veikti realiame pasaulyje. Išmanieji namų asistentai taip pat galėtų būti naudojami kaip ginklai, jei jie būtų susieti su išmania namų apsaugos sistema, tačiau tokiu atveju jų pritaikymas veikiau saugotų asmenų privatumą nuo įsibrovėlių, nei jį pažeistų. Galiausiai, nepastebimumas yra dar vienas aspektas, kuriuo bepiločiai orlaiviai skiriasi nuo išmaniųjų namų asistentų. Išmanieji namų asistentai yra matomi ir dažniausiai žinomi šeimos nariams, tuo tarpu bepiločiai orlaiviai gali būti maži ir suprojektuoti taip, kad būtų nepastebimi, leidžiant jiems slapta stebėti žmones ne tik namuose, bet ir už jų ribų.

Slapukai internete (cookies) renka informaciją apie vartotojų veiklą internete, pvz., naršymo istoriją, pirkimo įpročius ir svetainių lankomumą. Šie duomenys yra riboti virtualia erdve ir naršyklės kontekstu. Priešingai nei slapukai, dronai gali stebėti realų pasaulį, rinkdami duomenis apie fizinius veiksmus ir buvimo vietas, kas leidžia sujungti šiuos duomenis su internetiniais duomenimis ir sukurti išsamesnį naudotojo profilį. Ribos tarp virtualaus ir realaus pasaulio nyksta, kai sujungiami duomenys iš abiejų šaltinių, ko negalima atlikti vien naudojantis slapukais. Slapukų naudojimo mastas internetinėje erdvėje yra milžiniškas, ir jų pritaikymo galimybės virtualioje erdvėje yra plačios. Slapukai gali būti naudojami vartotojų naršymo internete patirčiai gerinti ir tuo pačiu rinkti daug duomenų apie jų elgesį virtualioje erdvėje. Tačiau, vėlgi, jais nerenkami duomenys realioje erdvėje. Dėl galimybės judėti realioje erdvėje bepiločių orlaivių panaudojimo galimybės yra kur kas platesnės. Jie gali būti naudojami įvairiose srityse, tokiose kaip paieška ir gelbėjimas, žemės ūkis, infrastruktūros priežiūra, saugumo užtikrinimas ir netgi kaip ginklai. Toks platus pritaikymo spektras leidžia jiems rinkti išsamesnius ir įvairiapusiškesnius duomenis nei slapukai. Stebėjimo intensyvumas pasitelkiant slapukus taip pat didelis, tačiau apsiriboja virtualioje erdvėje išgauta informacija. Dėl tos pačios priežasties slapukai taip pat nepasižymi tokia didele stebėjimo kampų įvairove kaip bepiločiai. Slapukai taip pat kaip ir bepiločiai orlaiviai pasižymi nepastebimumu. Dabartinis teisinis reguliavimas įpareigoja internetinių svetainių savininkus prašyti sutikimo vartotojų sutikimo slapukų naudojimui, tačiau žmonės tokių sutikimo prašymų naršydami internete gauna tiek daug, jog į jais renkamų duomenų turinį visai neturi laiko gilintis, todėl lengva ranka „atiduoda“ savo privatumą siekdami nepertraukiamai toliau naršyti internete. Šiuo aspektu bepiločiai gali būti pavojingesni už slapukus, nes pasižymi kitokio pobūdžio nepastebimumu. Netolimoje ateityje apie vabzdžio dydžio bepiločiais orlaiviais vykdomą stebėseną, nesant tinkamų reguliavimo priemonių, žmonės iš viso galėtų nežinoti. Slapukai gali būti naudojami kaip psichologinės manipuliacijos priemonės (ginklai), tačiau, priešingai nei bepiločiai orlaiviai, jie negali padaryti fizinio poveikio.

Taigi bepiločių orlaivių technologija dėl išskirtinių savybių, kuriomis nepasižymi nė viena iki šiol prieinama stebėsenos priemonė, sukuria puikią infrastruktūrą oportunistiniam informacijos rinkimui realiame pasaulyje. Šiame skyriuje identifikuotos pagrindinės priežastys – ribų tarp virtualaus ir realaus pasaulio nykimas, platus naudojimo mastas, stebėjimo intensyvumas, stebėjimo kampų įvairovė, galimybė tapti ginklu ir nepastebimumas – išryškina, kuo bepiločiai orlaiviai skiriasi nuo kitų privatumą galinčių pažeisti technologijų, tokių kaip išmanieji telefonai, CCTV kameros, socialinių tinklų platformos, išmanieji namų asistentai ir slapukai internete. Šios unikalios savybės leidžia bepiločiams orlaiviams rinkti informaciją plačiai, intensyviai ir nepastebimai, kas gali sukelti rimtas pasekmes asmens privatumui. Tinkamai nereglamentuotas jų naudojimas gali paveikti individų psichologiją, socialinių grupių ir skirtingų visuomenės sluoksnių elgseną, taip pat ir demokratinės santvarkos stabilumą. Todėl labai svarbu, kad bepiločių orlaivių naudojimas būtų reguliuojamas atsižvelgiant ne tik į grėsmę žmonių sveikatai ir gyvybei, bet ir realius pavojus, kylančius privatumui.

2. PRIVATUMO APSAUGA, KURIĄ NUMATO SPECIALUSIS BEPILOČIŲ ORLAIVIŲ REGULIAVIMAS

Atlikta privatumo istorinių ištakų analizė atskleidė, kaip skirtingai suprantama teisę į privatumą, o pateikta privatumo pažeidimų klasifikacija (1 schema) parodė priežastis, kylančias dėl bepiločių orlaivių naudojimo. Viena pagrindinių bepiločių orlaivių savybių, lemsiančių privatumo koncepcijos poslinkį, – jų teikiama galimybė stebėseną vykdyti be stebimojo žinios (nepastebimumas), dėl to stebimieji gali net neįtarti, kad kažkas naudodamasis bepiločiu orlaiviu pažeidinėja jų privatumą. Tai gali būti kliūtimi siekiant pasinaudoti pažeistos teisės gynybos būdais, tokiais kaip teisė kreiptis į teismą. Tam, kad tradicinės civilinės atsakomybės nuostatos veiktų, būtinos specialios taisyklės, kurios apribotų bepiločių orlaivių nepastebimumą iki tokio lygio, kad nukentėjusioji šalis privatumo pažeidimus galėtų pastebėti ir įrodyti, jog šie buvo įvykdyti. Tokios priemonės turėtų veikti prevenciškai, t. y. kuo mažiau galimybių stebėti asmenis paslapčia, tuo mažiau ir privatumo pažeidimų.

Šiame disertacijos skyriuje analizuojamos prevencinės privatumo apsaugos priemonės specialiuose bepiločių orlaivių reguliavimo dokumentuose bei šaltiniuose, jų tikslas – iš anksto užkirsti kelią privatumo pažeidimams. Atliekant privatumo pažeidimų tyrimą nagrinėjami ICAO, JARUS, ES ir JAV specialieji reguliavimo dokumentai. ICAO ir JARUS pasirinktos dėl jų svarbos tarptautiniam bepiločių orlaivių reguliavimui – jų priimti techniniai standartai dažnai tampa pagrindu nacionalinėms taisyklėms, kurios užtikrina vieningą bepiločių orlaivių naudojimo reguliavimą įvairiose valstybėse. Šie standartai padeda sukurti bendras gaires, kurios supaprastina tarptautinį dronų naudojimą ir didina reguliacinį suderinamumą. JAV ir ES pasirinktos dėl reikšmingų jų teisinių ir kultūrinių skirtumų: JAV teisė labiau orientuota į technologijų inovacijų skatinimą ir rinkos laisvę, o ES pabrėžia griežtą privatumo apsaugą ir valstybės reguliavimo svarbą. Tokiu pasirinkimu siekta atskleisti tiek stipriąsias, tiek silpnąsias skirtingų reguliavimo modelių puses.

Šis skyrius įgyvendina trečią disertacijos uždavinį. Pirmame šios dalies poskyryje aptariami galimi teisinių santykių reguliavimo būdai, kurie skaitytojui turėtų padėti geriau suprasti disertacijoje vartojamą reguliavimo sąvoką ir suvokti kiekvieno šioje dalyje analizuojamo šaltinio teisinę galią. Antras poskyris apibendrina tolesnio tyrimo metu analizuojamus šaltinius ir juose naudojamas bepiločių orlaivių klasifikacijas. Trečiame poskyryje identifikuojamos privatumo apsaugos priemonės, kurias numato specialusis bepiločių orlaivių reguliavimas ir kurios hipotetiškai galėtų sumažinti privatumo pažeidimų tikimybę; diskutuojama, kiek realiai kiekviena iš jų galėtų apsaugoti privatumą.

2.1. *Reguliavimo* samprata

A. Vaišvila teisinį reguliavimą yra apibrėžęs kaip tokią socialinio reguliavimo rūšį, arba formą, kada teisinis poveikis žmonių elgesiui yra daromas teisės normomis[240], tačiau disertacijoje vartojama plačiau apibrėžiama *reguliavimo* sąvoka, kuri apima ne tik formalų teisinį reglamentavimą. Remiantis užsienio autorių darbais, *reguliavimas* (angl. *regulation*) gali būti įvairių formų, į šią sąvoką patenka ne tik formalūs teisės aktai, bet ir vadinamoji negriežtoji teisė (angl. *soft law*)[241]. Kai kurie autoriai *reguliavimą* apibrėžia kaip atkaklų, sutelktą siekį pakeisti kitų elgesį pasitelkiant tam tikrus standartus ar tikslus, pvz., sukurti standartų nustatymo mechanizmus, surinkti informaciją ar modifikuoti elgesį[242]. Jacques'as Pelkmansas ir Andrea Renda yra išskyrę šešis reguliavimo intervencijos (angl. *regulatory intervention*) būdus, kurie yra susiformavę ES praktikoje. Teisės normos, kurias mini A. Vaišvila apibrėždamas teisinį reguliavimą, yra vienas iš reguliavimo būdų, tačiau į pokyčius rinkoje galima reaguoti ir mažesnės intervencijos reikalaujančiomis priemonėmis[243]. Formaliam teisiniam reguliavimui alternatyvūs būdai yra reguliavimas informuojant (angl. *regulation through information*), savireguliavimas (angl. *self-regulation*), jungtinis reguliavimas (angl. *co-regulation*), standartizavimas (angl. *standardization*) ir rinkos priemonės (angl. *market-based instruments*)[244]. 1 lentelėje apibendrintai pateikta reguliavimo rūšių taksonomija, ja bus vadovaujamasi ir toliau šiame skyriuje.

1 lentelė. *Teisinių santykių reguliavimo būdai*

TEISINIŲ SANTYKIŲ REGULIAVIMO BŪDAI				
	Apibrėžimas	**Praktiniai įgyvendinimo būdai**	**Valstybės intervencijos lygis**	**Privačių subjektų intervencijos lygis**
Reguliavimas informuojant	reguliavimo būdas, kurio tikslas paveikti vartotojų ir verslo subjektų elgesį padidinant rinkoje viešai prieinamą informacijos kiekį	informacinės kampanijos; informaciniai tinklaraščiai	aukštas	labai žemas

240 Alfonsas Vaišvila, *Teisės teorija* (Vilnius: Justitia, 2005).

241 Arie Rip, „De facto Governance of Nanotechnologies", *Futures of Science and Technology in Society,* (Wiesbaden: Springer Fachmedien Wiesbaden, 2018), 75–96, https://doi.org/10.1007/978-3-658-21754-9_5.

242 Roger Brownsword ir Morag Goodwin, *Law and the Technologies of the Twenty-first Century: Text and Materials* (Cambridge University Press, 2012); Julia Black, „Critical reflections on regulation", *Austl. J. Leg. Phil.* 27 (2002): 1.

243 Jacques Pelkmans ir Andrea Renda, „Does EU Regulation Hinder or Stimulate Innovation?", CEPS special report (Brussels: Centre for European Policy Studies, 2014).

244 *Ibid.*

Savireguliavimas	rinkos žaidėjų savanoriškai sukurti elgesio standartai	savanoriški susitarimai tarp rinkos dalyvių (ūkio subjektų, nevyriausybinių organizacijų, organizuotų grupių); elgesio kodeksai; bendrosios gairės	labai žemas	labai aukštas
Jungtinis reguliavimas	mechanizmas, kai teisės aktais nustatomi abstraktūs tikslai tam tikroje srityje pripažintiems veikėjams (ūkio subjektams, socialiniams partneriams, nevyriausybinėms organizacijoms ar asociacijoms), kuriais vadovaudamiesi standartus jie nusistato patys	privalomo pobūdžio teisės aktais nustatyti bendrieji principai	žemas	aukštas
Standartizavimas	reguliavimo metodas, kai formalaus reguliavimo galią turinti institucija suteikia mandatą vyriausybinei organizacijai kurti rekomendacinio pobūdžio standartus; į standartų kūrimo procesą organizacija įtraukia suinteresuotus fizinius ir juridinius asmenis	nacionalinės standartizavimo organizacijos rekomendacijos, komentarai, metodologijos	vidutinis	vidutinis
Rinkos priemonės	instrumentai, kuriais rinkos žaidėjams valstybė teikia pozityvią ar negatyvią piniginę paskatą arba nustato pagrindines žaidimo taisykles	parduodamos kompensacijos; parduodami leidimai; mokesčiai, rinkliavos; nuosavybės ir atsakomybės taisyklės; limitai kainoms ir (arba) kiekiams (licencijos, kvotos ir pan.)	aukštas	žemas
Formalus reguliavimas	detalūs privalomo pobūdžio reikalavimai, įtvirtinti teisės aktuose, kurie nustato elgesio taisykles individualiai neapibrėžtai asmenų grupei	reglamentai; direktyvos; įstatymai; kodeksai; ministrų įsakymai	labai aukštas	labai žemas

Nedideli bepiločiai orlaiviai išpopuliarėjo neseniai, tai palyginti naujas reiškinys, todėl jų formalus reguliavimas nėra plačiau apibrėžtas. Disertacijos autoriaus nuomone, šiuo metu reikėtų vadovautis platesniu *reguliavimo* apibrėžimu, kuris leistų susidaryti aiškesnį vaizdą organizacijų, turinčių įtaką bepiločių orlaivių rinkoje, ir jų siūlomas privatumo apsaugos priemones.

2.2. Specialusis bepiločių orlaivių reguliavimas

2.2.1. Šaltiniai

Šiuo metu pagrindinį vaidmenį kuriant bepiločių orlaivių teisinį reguliavimą tarptautiniu mastu atlieka dvi organizacijos – ICAO ir JARUS.

ICAO yra Jungtinių Tautų institucija, įkurta 1944 m., jos tikslas – administruoti klausimus, susijusius su Tarptautine civilinės aviacijos konvencija (arba Čikagos konvencija). Ją pasirašė 193 valstybės narės, tarp jų ir Lietuva. ICAO iki šiol yra publikavusi pavyzdinius bepiločių orlaivių reglamentus 101, 102 ir 149, taip pat juos konkretizuojančius patariamuosius aplinkraščius (101-1, 102-1 ir 102-23). ICAO rekomenduoja valstybėms narėms juos naudoti kaip šablonus priimant, papildant ar keičiant nacionalinį bepiločių orlaivių teisinį reglamentavimą[245].

Kita svarbi organizacija, kurianti bepiločių orlaivių teisinį reguliavimą, yra ekspertų grupė JARUS. Ji vienija įvairių pasaulio šalių ekspertus ir nacionalines valdžios institucijas (2019 m. rugpjūčio mėn. JARUS turėjo 61 narį). Šios tarptautinės grupės tikslas – sukurti bepiločių orlaivių reglamentavimo standartus ir teikti rekomendacinę medžiagą, skirtą palengvinti nacionalinių bepiločių orlaivių teisės aktų kūrimą. Nuo 2012 m. JARUS yra publikavusi daugybę išsamių bepiločių orlaivių saugumo ir sertifikavimo reikalavimus aptariančių rekomendacijų[246].

Europoje kuriant bepiločių orlaivių reguliavimą svarbiausias vaidmuo tenka trims organizacijoms: Europos Komisijai, kuri yra ES vykdomoji institucija, Europos aviacijos saugumo agentūrai (EASA), kuri atsakinga už aviacijos saugumą ES, ir SESAR JU, t. y. bendras viešojo ir privataus sektorių projektas. Visų šių institucijų tikslas – sukurti naujovišką, automatizuotą oro eismo valdymo (angl. *Air Traffic Management* – ATM) sistemą, į kurią būtų įtraukti ir bepiločiai orlaiviai[247].

Naujos ATM sistemos sukūrimas gali užtrukti net iki 2050 m.[248], o bepiločiai orlaiviai įvairiais tikslais plačiai naudojami jau dabar, todėl bepiločių oro eismo valdymo (UTM) sistemai ES planuoja skirti daugiau dėmesio[249]. Bepiločių orlaivių saugios integracijos į oro erdvę iniciatyva svarbiausiuose ES dokumentuose įvardijama pavadinimu „U-space“. Šios sistemos tikslas yra oro erdvės, kurioje skraidys bepiločiai orlaiviai, naudojimą palaipsniui padaryti kuo labiau automatizuotą ir suskaitmenintą, tokiu būdu suteikiant galimybę joje skrydžius vykdyti vienu metu daugybei bepiločių orlaivių. ES „U-space“ planuoja įdiegti keturiais etapais.

---

245 ICAO model UAS regulations part 101 and 102, (2020); ICAO model UAS regulations part 149, (2020); ICAO Advisory Circular (AC) 101-1, (2020); ICAO Advisory Circular (AC) 102-1, (2020); ICAO Advisory Circular (AC) 102-23, (2020).

246 JARUS tinklalapis, žiūrėta 2020 m. birželio 22 d., http://jarus-rpas.org/publications

247 SESAR Joint Undertaking, „European ATM master plan“ (Publications Office of the European Union, 2020).

248 Europäische Kommission ir Europäische Kommission, sud., *Flightpath 2050: Europe's Vision for Aviation; Maintaining Global Leadership and Serving Society's Needs; Report of the High-Level Group on Aviation Research,* Policy / European Commission (Luxembourg: Publ. Off. of the Europ. Union, 2011).

249 *Ibid.,* 65.

Per pirmąjį numatoma padėti sistemos pamatus – identifikuoti bepiločius orlaivius, jų valdytojus ir informuoti juos apie zonas, kuriose skrydžius vykdyti draudžiama[250]. Jau parengti trys dokumentai, atsiradę iš bendrų EASA, SESAR JU ir Europos Komisijos pastangų: Reglamentas (ES) 2018/1139[251] (toliau – Bendrasis aviacijos reglamentas), Reglamentu (ES) 2019/945[252] (toliau – Deleguotasis reglamentas), kuris numato techninius reikalavimus bepiločiams orlaiviams ir jų priedams, ir Reglamentu (ES) 2019/947[253] (toliau – Įgyvendinimo reglamentas), kuris numato bepiločių orlaivių naudojimo apribojimus nuotoliniams pilotams. Lietuva, kaip ES valstybė, ES reglamentus privalo taikyti tiesiogiai, todėl analizėje ji neišskiriama kaip atskira jurisdikcija.

JAV už bepiločių orlaivių reglamentavimą atsakinga FAA, kuri 2016 m. publikavo Nedidelių bepiločių orlaivių naudojimo ir sertifikavimo taisykles[254]. Jomis prie CFR 14 antraštės pridėtas 107 skyrius, kuriame aptariami nedidelių bepiločių orlaivių naudojimo ypatumai[255].

Visi su bepiločiais orlaiviais susiję ICAO bei JARUS išleisti dokumentai apsiriboja reikalavimais bepiločių orlaivių sertifikavimui bei saugiam naudojimui, tačiau neapima tokių aspektų kaip privatumas, kurį, ICAO manymu, valstybės turėtų reguliuoti nacionaliniu mastu[256]. JARUS viename savo dokumentų yra minėjusi, kad dėl bepiločių orlaivių naudojimo kylančios grėsmės gali būti sietinos ne tik su saugumu, bet ir su nuosavybe, privatumu, kibernetiniu saugumu, aplinkos apsauga, tačiau nuomonės dėl šių rizikų reglamentavimo gali labai skirtis, priklausomai nuo kiekvienos valstybės kultūrinių vertybių. Todėl JARUS apsiriboja tik rekomendacijomis, skirtomis saugiam bepiločių orlaivių naudojimui reglamentuoti[257]. JAV nedidelių bepiločių orlaivių naudojimą reguliuojančios taisyklės taip pat tiesiogiai nepaliečia su privatumu susijusių problemų. FAA nurodo, jog privatumo gairių galima tikėtis netolimoje ateityje[258], o šiuo metu bepiločių orlaivių pilotai raginami

---

250 *Ibid.,* 66.

251 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91.

252 „2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų“, OJ L 152, 2019 m. birželio 11 d., 1–40.

253 „2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos“, OL L 152, 2019 m. birželio 11 d., 45–71.

254 Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems“, FAA–2015–0150, *Federal Register,* 81, 124 (2016): 42064–42214.

255 JAV Federalinių teisės aktų kodeksas, 14 antraštė, 107 dalis.

256 ICAO model UAS regulations part 101 and 102, *supra note,* 22: 1.

257 JARUS UAS Operational Categorization, *supra note,* 22.

258 „Fact Sheet – Small Unmanned Aircraft Regulations (Part 107)“, žiūrėta 2020 m. liepos 28 d., https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516.

vadovautis JAV nacionalinės telekomunikacijų ir informacijos administracijos (NTIA) paskelbtomis pagrindinių bepiločių orlaivių rinkos suinteresuotų šalių suformuotomis gerosios praktikos gairėmis[259] (toliau – Gerosios praktikos gairės). ES nurodo, jog bepiločių orlaivių reglamentai yra skirti užtikrinti ne tik skrydžių bepiločiais orlaiviais saugumą, bet ir duomenų apsaugą bei privatumą. Nors ES reglamentuose nėra atskiros dalies privatumui ir duomenų apsaugai, bet poreikis šias teises apsaugoti minimas dažnai[260].

Taigi analizuojant specialųjį bepiločių orlaivių reguliavimą galima įžvelgti tris skirtingus požiūrius į privatumo reguliavimą. ES privatumo ir asmens duomenų apsauga *expressis verbis* įtraukta į formalų bepiločių orlaivių reguliavimą. JAV privatumo apsaugos į formalų bepiločių orlaivių reguliavimą neįtraukia, bet iš dalies aptaria privatumo apsaugą bendrojo reguliavimo šaltiniuose. ICAO ir JARUS pasirenka expressis verbis privatumo apsaugos nereguliuoti. Nepaisant šių skirtumų, manytina, jog net ir laikantis reguliavimo, kur *expressis verbis* nėra reguliuojamas privatumas, gali būti priemonių, kurios prie privatumo apsaugos gali prisidėti netiesiogiai. Taigi, privatumo apsaugos priemonių bus ieškoma nagrinėjant detaliau kiekvienos iš keturių institucijų specialųjį bepiločių orlaivių reguliavimą.

Šiame skyriuje analizuojami jau minėti specialūs reguliavimo šaltiniai, nustatantys taisykles, kaip naudoti bepiločius orlaivius tarptautiniu, ES ir JAV mastu. Kuriant pasirinktus šaltinius reikšmingai prisidėjo ne tik institucijos ir organizacijos, bet ir privatūs bepiločių orlaivių rinkos dalyviai. Netgi formalūs reguliavimo šaltiniai, galiojantys ES bei JAV, buvo priimti tik po ilgai trukusių viešų konsultacijų su privačiais subjektais. Todėl šaltiniuose aptartos priemonės turėtų patikimai atskleisti visą kiekvienos jurisdikcijos viešų ir privačių subjektų įdirbį, siekiant sureguliuoti bepiločių orlaivių naudojimą. Šaltiniai, naudoti analizei, apibendrintai pateikti 2 lentelėje.

2 lentelė. *Specialieji bepiločių orlaivių reguliavimo šaltiniai*

259 „Voluntary Best Practices for UAS Privacy, Transparency, and Accountability“ (National Telecommunications and Information Administration, 2016).

260 Žr. Reglamento (ES) 2019/945 preambulės 2 punktą, Reglamento (ES) 2019/947 preambulės 14, 16, 18–21 punktus, 2 straipsnio 4 punktą, 12 straipsnio 2 dalies c punktą.

SPECIALIEJI BEPILOČIŲ ORLAIVIŲ REGULIAVIMO ŠALTINIAI			
Jurisdikcija	**Atsakingos institucijos**	**Šaltiniai**	**Reguliavimo būdas**[261]
Tarptautinė	ICAO	*ICAO model UAS regulations part 101 and 102*	standartizavimas
		ICAO model UAS regulations part 149	
		ICAO Advisory Circular (AC) 101-1	
		ICAO Advisory Circular (AC) 102-1	
		ICAO Advisory Circular (AC) 102-23	
	JARUS	*JARUS UAS Operational Categorization*	standartizavimas
		JARUS Recommendation for remote pilot competency (RPC) for UAS operations in Category A (open) and Category B (specific)	
		JARUS FCL Recommendation	
Europos Sąjunga	Europos Komisija, EASA, SESAR JU	2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, kuriuo įsteigiama ES aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES bei 2014/53/ES, panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91	formalus reguliavimas
		2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų	
		2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos	

261 Pagal 1 lentelėje numatytus teisinių santykių reguliavimo būdus.

Jungtinės Amerikos Valstijos	FAA	*„Registration and Marking Requirements for Small Unmanned Aircraft“, Final interim rule, Federal Aviation Administration (FAA), FAA-2015-7396, 80 FR 78593, 2015-12-16*	formalus reguliavimas
		„Operation and Certification of Small Unmanned Aircraft Systems“, Final rule, Federal Aviation Administration (FAA), FAA–2015–0150, 81 FR 42063, 2016-06-28	
		„Remote Identification of Unmanned Aircraft“, Final rule, Federal Aviation Administration (FAA), FAA-2019-1100, 86 FR 4390, 2021-01-15	
		Title 14 CFR Part 48, Registration and Marking Requirements for Small Unmanned Aircraft	
		Title 14 CFR Part 89, Remote Identification of Unmanned Aircraft	
		Title 14 CFR Part 107, Small Unmanned Aircraft Systems	
		FAA Reauthorization Act of 2018	
		Title 49 U.S.C. § 44809, Exception for Limited Recreational Operations of Unmanned Aircraft	
		AC 107-2, Small Unmanned Aircraft Systems (Small UAS)	standartizavimas
		AC 91-57C, Exception for Limited Recreational Operations of Unmanned Aircraft	
		„Voluntary Best Practices for UAS Privacy, Transparency, and Accountability“, National Telecommunications and Information Administration, 2016	jungtinis reguliavimas

Iš šaltinių, kurie analizuojami šiame skyriuje, matyti, kad kiekvienos iš pasirinktų institucijų reguliavimo šaltiniuose bepiločiai orlaiviai arba jais vykdomi skrydžiai yra skirstomi į tipus ir kategorijas. Prieš pradedant nagrinėti šaltiniuose esančias privatumo apsaugos priemones ir siekiant išvengti neaiškumų, vertėtų apžvelgti, kokius klasifikavimo variantus pasirinko analizuojamos organizacijos. Apie tai detaliau kitame poskyryje.

2.2.2. Bepiločių orlaivių klasifikacijos

Išsamiausiai bepiločius orlaivius ir jais vykdomus skrydžius skirsto ES. ES reglamentai bepiločius pagal rizikos lygį skirsto į atvirąją, specialiąją ir sertifikuotąją klases. Atviroji yra papildomai dalijama į A1, A2 ir A3 pakategores. Atvirosios kategorijos bepiločiai orlaiviai dar skirstomi į penkias klases (C0, C1, C2, C3, C4) pagal masę. ES klasifikacija pateikta 3 lentelėje.

3 lentelė. *Bepiločių orlaivių klasifikacija laikantis ES reguliavimo*

<table>
<tr><th colspan="5">Bepiločių orlaivių klasifikacija laikantis ES reguliavimo</th></tr>
<tr><th>Kategorijos</th><th>Pakategorės</th><th>Klasės (pagal masę)</th><th>Svoris (MTOM)</th><th>Reguliavimas</th></tr>
<tr><td rowspan="5">Atviroji (žema rizika)</td><td rowspan="2">A1 – galima skristi virš žmonių, tačiau ne virš minių</td><td>C0</td><td>< 250 g</td><td rowspan="4">minimalus</td></tr>
<tr><td>C1</td><td>< 290 g</td></tr>
<tr><td>A2 – galima skristi saugiu atstumu nuo žmonių</td><td>C2</td><td>< 4 kg</td></tr>
<tr><td rowspan="2">A3 – galima skristi vietovėje, kur pagrįstai tikėtina, jog nebus pakenkta pašaliniams asmenims, ir bus laikomasi saugaus atstumo nuo miestų</td><td>C3</td><td rowspan="2">< 25 g</td></tr>
<tr><td>C4</td></tr>
<tr><td>Specialioji (vidutinė rizika)</td><td>-</td><td>-</td><td>-</td><td>nepriklausomai vertinamas nacionalinės aviacijos organizacijos</td></tr>
<tr><td>Sertifikuotoji (didelė rizika)</td><td>-</td><td>-</td><td>-</td><td>taikomas galiojantis aviacijos reguliavimas</td></tr>
</table>

JARUS pateikta bepiločių orlaivių klasifikacija praktiškai identiška ES skirstymui. Vienintelis skirtumas yra tas, kad JARUS kiek kitaip juos skirsto pagal masę. JARUS klasifikacija pateikta 4 lentelėje.

4 lentelė. *Bepiločių orlaivių klasifikacija laikantis JARUS reguliavimo*

Bepiločių orlaivių klasifikacija laikantis JARUS reguliavimo			
Kategorijos	**Pakategorės**	**Svoris (MTOM)**	**Reguliavimas**
A – atviroji (žema rizika)	A1 – galima skristi virš žmonių, tačiau ne virš minių	< 250 g	minimalus
	A2 – galima skristi saugiu atstumu nuo žmonių	250 g–4 kg	
	A3 – galima skristi vietovėje, kur nekeliamas pavojus žmonėms, nedalyvaujantiems operacijoje ir saugiu atstumu nuo tankiai apgyvendintų zonų ribų	250 g–25 kg	
B – specialioji (vidutinė rizika)	–	–	nepriklausomai vertinamas nacionalinės aviacijos organizacijos
C – sertifikuotoji (didelė rizika)	–	–	taikomas galiojantis aviacijos reguliavimas

ICAO bepiločius orlaivius skirsto tik į dvi kategorijas – atvirąją ir specialiąją. Atvirosios kategorijos skrydžiai gali būti vykdomi bepiločiais orlaiviais, kurių masė mažesnė kaip 25 kg, o visi kiti skrydžiai, kurie nepatenka į atvirąją kategoriją, priskiriami specialiajai, tarp jų ir skrydžiai bepiločiais orlaiviais, kurių masė didesnė kaip 25 kg. ICAO klasifikacija pateikta 5 lentelėje.

5 lentelė. *Bepiločių orlaivių klasifikacija laikantis ICAO reguliavimo*

Bepiločių orlaivių klasifikacija laikantis ICAO reguliavimo		
Kategorijos	**Svoris (MTOM)**	**Reguliavimas**
Atviroji	< 25 kg	iki 15 kg tik minimalūs reikalavimai, keliami jų valdymui; nuo 15 kg iki 25 kg bepiločiai orlaiviai turi atitikti nacionalinės aviacijos organizacijos reikalavimus, keliami minimalūs reikalavimai jų valdymui
Specialioji	> 25 kg	turi būti išduotas nacionalinės aviacijos organizacijos bepiločio orlaivio leidimas arba bepiločio orlaivio operatoriaus sertifikatas

JAV reguliavimas aiškaus skirstymo į atskiras kategorijas nei pagal bepiločių orlaivių svorį, nei pagal jų pavojingumą nenumato. Vis dėlto rekreaciniams skrydžiams gali būti taikomos specialios taisyklės, todėl pagal JAV reguliavimą nedidelių bepiločių orlaivių (iki 25 kg) skrydžius galima būtų klasifikuoti į rekreacinius ir komercinius. JAV reguliavimas, skirtingai nei kitų jurisdikcijų, šiuo metu neapima bepiločių orlaivių, kurių svoris didesnis kaip 25 kg. Tokiems bepiločiams pagal JAV reguliavimą galėtų būti taikomos nebent bendros aviacijos taisyklės. JAV klasifikacija pateikta 6 lentelėje.

6 lentelė. *Bepiločių orlaivių klasifikacija laikantis JAV reguliavimo*

Bepiločių orlaivių klasifikacija laikantis JAV reguliavimo		
Kategorijos	**Svoris (MTOM)**	**Reguliavimas**
Rekreaciniai skrydžiai	< 25 kg	galima vykdyti skrydžius tiek pagal specialiąsias taisykles, skirtas rekreaciniams bepiločių orlaivių skrydžiams[262], tiek pagal CFR 14 antraštės 107 dalį[263]
Komerciniai skrydžiai	< 25 kg	galima vykdyti skrydžius pagal CFR 14 antraštės 107 dalį[264]

Bepiločiai orlaiviai, keliantys didžiausią grėsmę privatumui, yra tie, kuriuos gali įsigyti vidutinis vartotojas, kurie keltų mažai triukšmo ir kurie būtų sunkiau pastebimi. Tokius bruožus geriausiai atitinka mažų gabaritų bepiločiai orlaiviai. Nagrinėjamuose dokumentuose laikomasi nuostatos, kad nedideli bepiločiai orlaiviai yra tie, kurių svoris ne didesnė kaip 25 kg. JAV šiuo metu reglamentuoja tik nedidelių bepiločių orlaivių naudojimą. ES reglamentai bei tarptautinės rekomendacijos nustato ir didesnių bepiločių orlaivių naudojimą, kurių svoris viršija 25 kg. Nors didesni bepiločiai orlaiviai reikšmingos grėsmės privatumui nekelia, vis dėlto jų reguliavimo nereikėtų palikti nuošalėje, kadangi net ir didesnių bepiločių orlaivių naudojimo taisyklėse gali būti priemonių, kurias pritaikius nedideliems bepiločiams orlaiviams privatumo apsauga didėtų. Todėl toliau analizuojamos ne tik priemonės, skirtos nedideliems bepiločiams orlaiviams, bet ir reikalavimai, taikomi didesniems bepiločiams orlaiviams.

262 *FAA Reauthorization Act of 2018.*
263 CFR section 14, part 107.
264 *Ibid.*

2.3. Privatumo apsaugos priemonės, kurias numato specialusis bepiločių orlaivių reguliavimas

Atlikus preliminarią reguliavimo šaltinių analizę matyti, kad gali būti priemonių, kurios užkirstų kelią privatumo pažeidimams. Siekiant įvertinti kiekvienos iš jų veiksmingumą, būtina nuodugnesnė analizė. Keliama hipotezė, kad privatumo pažeidimų dažnumą galėtų sumažinti šios specialiajame bepiločių orlaivių reguliavime aptartos prevencines priemonės:

- reikalavimas laikytis atstumo;
- reikalavimas informuoti ar gauti sutikimą;
- registracijos reikalavimas;
- reikalavimas kaupti įrašus;
- kvalifikacijos reikalavimai, keliami bepiločių orlaivių pilotams;
- reikalavimas atlikti rizikos vertinimą;
- nuotolinio identifikavimo priedai;
- geografinio orientavimo priedai;
- duomenų perdavimo ryšio linijos saugumo užtikrinimas;
- reikalavimas bepiločius orlaivius gaminti su žibintais.

Hipotezei patikrinti kiekviena priemonė bus analizuojama atskirai. Bus komentuojamos ir lyginamos šias priemones aptariančios specialių reguliavimo šaltinių nuostatos. Jas išanalizavus pateikiamos įžvalgos, siekiant atsakyti į klausimą, ar atitinkama priemonė galėtų apsaugoti privatumą. Galiausiai pateikiami siūlymai, kaip konkrečios priemonės galėtų būti tobulinamos.

2.3.1. Reikalavimas laikytis atstumo

Viena iš nuostatų, galinti apsaugoti privatumą, yra reikalavimas laikytis atstumo. Šiuolaikinės vaizdo kameros yra stipriai patobulėjusios, jos turi didelę vaizdo raišką ir mikrofonus, atpažįstančius garsą per didelį atstumą. Kameros raiška dažniausiai būna tiesiogiai proporcinga jos dydžiui, šiuo metu mažiausi bepiločiai orlaiviai neturi tokių pačių filmavimo ir fotografavimo galimybių kaip dideli ir brangūs komerciniai bepiločiai. Tas pats tinka ir garso įrašymo aparatūrai – pažangią kryptinių mikrofonų technologiją, kuri fiksuotų garsą dideliu atstumu, šiuo metu galima būtų pritaisyti nebent prie didelių bepiločių orlaivių[265]. Tokio atstumo, iš kurio tiesiog nebūtų matyti žmonių veidai arba nesigirdėtų jų pašnekesiai dėl techninių vaizdo kameros ar mikrofonų galimybių, laikymasis vykdant skrydį bepiločiu orlaiviu turėtų padėti išvengti daugelio privatumo pažeidimų[266]. Jie ir

---

265 „Long range directional microphone X64ACS specifications“, žiūrėta 2022 m. gruodžio 16 d., http://ampflab.com/long-range-directional-microphone-X64ACS.html; (mažiausias tinklalapyje reklamuojamas profesionalus kryptinis mikrofonas, gebantis fiksuoti garsą iš 150 m atstumo, sveria 3 kg).

266 Galima būtų išvengti stebėsenos, agregavimo, identifikavimo ir saugumo neužtikrinimo pažeidimų. Atidengimo pažeidimo Atidengimo pažeidimui ne visuomet svarbus individo identifikavimo faktas. Šis pažeidimas gali pasireikšti nufilmuoto asmens psichologine kančia, nesaugumo jausmu.

toliau galėtų rinkti duomenis, jei jų vaizdo medžiagoje matytųsi tik žmonių siluetai, o garso medžiagoje – nereikšmingas triukšmas. Ar tokią privatumo apsaugą užtikrina dabartinis specialusis bepiločių orlaivių reguliavimas?

ICAO savo pavyzdiniuose reglamentuose numato draudimą skrydžius vykdyti bepiločiu orlaiviu arčiau kaip 30 m atstumu (matuojant horizontaliai) nuo asmens, kuris nedavė sutikimo, ir draudimą vykdyti skrydžius virš nuosavybės teise kitiems asmenims priklausančių objektų, nebent yra gautas savininko sutikimas[267]. Net jeigu asmuo sutinka, kad virš ar šalia jo būtų vykdomas skrydis, bepilotis orlaivis vis vien nuo jo turi laikytis ne mažesnio kaip 15 m horizontalaus atstumo[268].

JARUS rekomendacijos konkretaus atstumo, kurio nuo pašalinių asmenų turėtų laikytis bepilotis orlaivis, nenumato, tik nurodo, jog jo pilotas turėtų laikytis saugaus atstumo nuo žmonių, nuosavybės objektų, antžeminių ir oro transporto priemonių. Vadovaujantis JARUS, bepiločiais orlaiviais, kurių svoris yra nuo 250 g iki 4 kg, neturėtų būti leidžiama skristi virš žmonių sambūrių, o bepiločiais orlaiviais, kurių svoris yra 4–25 kg, skrydžiai turėtų būti vykdomi laikantis saugaus atstumo nuo tankiai apgyvendintų vietovių ribų ir nekeliant pavojaus pašaliniams asmenims[269].

Laikantis ES reglamentavimo, atstumas priklauso nuo bepiločio orlaivio svorio ir pavojingumo lygio. Bepilotis orlaivis, kurio svoris nesiekia 250 g (A1 pakategorė, C0 klasė), griežtai apibrėžto atstumo laikytis neprivalo, juo skrydžius galima vykdyti net ir virš pašalinių asmenų, tik reikia vengti skristi virš žmonių sambūrių[270]. Bepiločiams orlaiviams, kurių svoris yra 250–900 g (A1 pakategorės, C1 klasė), griežtai apibrėžto atstumo nuo asmenų laikytis neprivaloma, tačiau jais negalima skristi žmonėms virš galvų, o tuo atveju, jeigu bepilotis orlaivis kartais netikėtai atsidurtų virš pašalinių asmenų, nuotolinis pilotas privalo užtikrinti, kad jis virš asmenų skristų kuo trumpiau[271]. Bepiločiais orlaiviais, kurių svoris yra nuo 900 g iki 4 kg (A2 pakategorė, C2 klasė), galima skristi nuo pašalinių asmenų ne mažesniu kaip 30 m horizontaliu atstumu arba 5 m horizontaliu atstumu, jeigu įjungta mažojo greičio režimo funkcija, ir dar prieš skrydį įvertinus oro sąlygas, bepiločio orlaivio eksploatacines savybes, vietovės, virš kurios skraidoma, atskirtį.

---

267 *ICAO model UAS regulations* part 101 and 102, *supra note,* 22, 101.25 straipsnis, a dalis, 1 punktas, i pastraipa, 13.

268 *ICAO model UAS regulations* part 101 and 102, *supra note,* 22, 101.35 straipsnis, d dalis, 15.

269 „JARUS Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, 2019-07-11, http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_14_ops_cat_a_b_edition1.0.pdf, skyriaus „UAS.OPA.50 Requirements applicable to UAS Operations in subcategory A1“, 2 dalies b punktas; skyriaus „UAS.OPA.60 Requirements applicable to UAS operations in subcategory A2“ 2 dalies c punktas; skyriaus „UAS.OPA.70 Requirements applicable to UAS Operations in subcategory A3“ 2 dalies d ir e punktai.

270 Reglamento (ES) 2019/947 priedo A dalies „UAS.OPEN.020. UAS naudojimas A1 pakategorės skrydžiams vykdyti“ skyriaus 2 punktas.

271 Reglamento (ES) 2019/947 priedo A dalies „UAS.OPEN.020. UAS naudojimas A1 pakategorės skrydžiams vykdyti“ skyriaus 1 punktas.

Tokio dydžio bepiločiais orlaiviais neleidžiama skristi nei žmonėms virš galvų, nei virš žmonių sambūrių[272]. Bepiločiais orlaiviais, kurių svoris yra 4–25 kg (A3 pakategorė, C3, C4 klasės), skrydžius galima vykdyti 150 m horizontaliu atstumu nuo gyvenamosios, komercinės, pramoninės arba pramoginės paskirties zonų, taigi toli nuo pašalinių asmenų[273].

JAV reglamentavimas konkretaus horizontalaus atstumo, kurio bepilotis orlaivis turėtų laikytis nuo pašalinių asmenų, nenumato, tačiau draudžia bet kokius skrydžius virš pašalinių asmenų, nebent šie, virš kurių vykdomas skrydis, yra po stogu[274]. Nors oficialiame bepiločių orlaivių reglamentavime privalomos nuostatos neskristi virš privačios nuosavybės objektų nėra, JAV Gerosios praktikos gairėse nurodoma, jog bepiločių orlaivių pilotai, negavę savininko leidimo, turėtų vengti skristi virš privačios nuosavybės objektų[275].

Atlikus visų pasirinktų jurisdikcijų reguliavimo analizę, galima išskirti tris kriterijus, susijusius su reikalavimu laikytis atstumo, t. y.: 1) numatomas konkretus atstumas, kurio privalo laikytis bepiločio orlaivio pilotas nuo pašalinių asmenų ar nuosavybės objektų; 2) numatoma bendra pareiga laikytis saugaus atstumo; 3) nenumatomas joks konkretus atstumas, kurio bepiločio orlaivio pilotas turėtų laikytis nuo pašalinių asmenų. Šiuo atveju akivaizdu, kad privatumo apsaugą gali suteikti tik pirmas kriterijus, kuriuo vadovaujasi ICAO ir ES (taiko bepiločiams orlaiviams, kurių svoris nuo 900 g iki 25 kg), nes jis aiškiai nustato ribas, kurių bepiločio orlaivio valdytojas negali peržengti. Antrą kriterijų atskleidžia JARUS rekomendacijos, kurios privatumo klausimų nenagrinėja, todėl numato tik pareigą laikytis saugios distancijos, bet ne atstumo, užtikrinančio pašalinių asmenų privatumą. Vis dėlto net ir pakoregavus šį kriterijų, kaip numatantį pareigą laikytis tokio atstumo, kuris nepažeistų pašalinių asmenų privatumo, tikėtina, jog toks jo neapibrėžtumas leistų bepiločių orlaivių pilotams piktnaudžiauti, kaip ir tuo atveju, jei atstumo laikymasis būtų apskritai nenumatomas. Trečias kriterijus, kurį bent jau šiuo metu yra pasirinkusios taikyti JAV ir ES bepiločiams orlaiviams, sveriantiems mažiau negu 900 g, jokios privatumo apsaugos nesuteikia, nes horizontalaus apribojimo vykdyti skrydžius per atstumą nuo pašalinių asmenų tiesiog nėra. Kadangi nei antras, nei trečias kriterijai nebūtų veiksmingi privatumui apsaugoti, toliau analizuojamas pirmasis.

Konkretus atstumas nuo stebimo individo iki bepiločio orlaivio kameros galėtų apsaugoti privatumą tuo atveju, jeigu naudojant veido atpažinimo įrangą iš bepiločiu orlaiviu užfiksuotų nuotraukų būtų neįmanoma patikimai nustatyti žmogaus tapatybės, o iš įrašyto garso būtų neįmanoma suprasti pokalbio esmės. Tada reikia nuspręsti, koks turėtų būti tas tobulas atstumas?

---

272 Reglamento (ES) 2019/947 priedo A dalies „UAS.OPEN.030. UAS naudojimas A2 pakategorės skrydžiams vykdyti“ skyriaus 1 punktas.

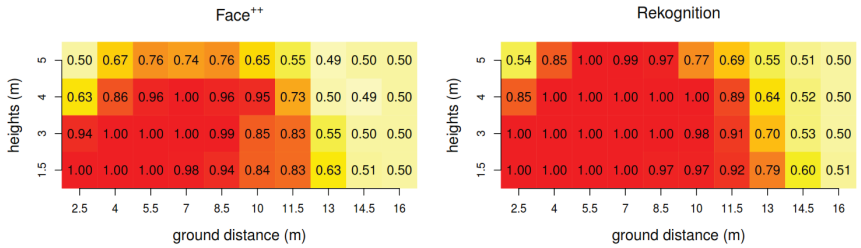
273 Reglamento (ES) 2019/947 priedo A dalies „UAS.OPEN.040. UAS naudojimas A3 pakategorės skrydžiams vykdyti“ skyrius.

274 JAV Federalinių teisės aktų kodeksas, 14 antraštė, 107.39 straipsnis.

275 „Voluntary Best Practices for UAS Privacy, Transparency, and Accountability“, *supra note,* 263: 8.

Į šio klausimo vieną aspektų (vaizdo įrašymo atstumą) atsakymą gali pateikti H. J. Hsu ir K. T. Chen[276] atliktas tyrimas, kuriame simuliuojant skrydį bepiločiu orlaiviu įvairiais atstumais ir aukščiais nuo stebimo individo buvo daromos nuotraukos. Vėliau jos analizuotos naudojant dvi populiarias veido atpažinimo programines įrangas („Face++“ ir „ReKognition“). Taip buvo vertinama, kokiu atstumu ir kokiame aukštyje darytos nuotraukos leido patikimai nustatyti stebimo individo tapatybę. Tyrimas parodė, kad veido atpažinimo sėkmė labai priklauso nuo naudojamos vaizdo kameros parametrų (pvz., skiriamosios gebos, suspaudimo laipsnio), kitaip tariant, kuo geresnė vaizdo kamera, tuo geresni rezultatai. Reikšmingą poveikį rezultatams darė ir tai, kokiu kampu nuotrauka buvo daroma, t. y. geriausi rezultatai gauti, kai nuosvyrio kampas (angl. *angle of depression*) mažiausias. Pvz., tyrimui naudota vaizdo kamera patikimiausius veido atpažinimo rezultatus pavyko gauti tada, kai fotografuota iš ne didesnio kaip 13 m atstumo, o skrydžio aukštis siekė 1,5 m. Skrydžio aukščiui didėjant, atstumas, iš kurio pavyko gauti patikimus rezultatus, mažėjo, pvz., 5 m aukštyje patikimus rezultatus pavyko gauti tik 8,5 m atstumu (žr. 2 schema[277]).

2 schema. Veido atpažinimo patikimumas vykdant skrydžius dronais



Nors H.-J. Hsu ir K.-T. Chen straipsnyje nurodyti konkretūs atstumai ir aukščiai, iš kurių darytos nuotraukos nebebuvo patikimos stebimų asmenų tapatybei nustatyti, tačiau vadovautis vien skaičiais negalima, nes šis tyrimas atliktas 2015 m., o nuo to laiko tiek bepiločių orlaivių vaizdo kamerų, tiek veido atpažinimo programinės įrangos galimybės galėjo reikšmingai patobulėti. Kita vertus, iš atlikto tyrimo matyti, kad atstumas, kurio bepilotis orlaivis privalėtų laikytis nuo stebimo individo, turėtų priklausyti nuo tokių kintamųjų: 1) bepiločio orlaivio vaizdo kameros parametrų, 2) veido atpažinimo programinės įrangos pažangumo ir 3) nuosvyrio kampo (skrydžio aukščio).

276 Hwai-Jung Hsu ir Kuan-Ta Chen, „Face recognition on drones: Issues and limitations“, *Proceedings of the first workshop on micro aerial vehicle networks, systems, and applications for civilian use* (2015): 39–44.

277 *Ibid.*, 6.

Garso įrašymo atstumą, kuris apsaugotų privatumą, nustatyti dar sudėtingiau. Fiksuojamo garso kokybė priklauso nuo tokių kintamųjų: bepiločio orlaivio variklio ir rotorių skleidžiamo garso, aplinkos, kurioje garsas įrašinėjamas, triukšmo lygio, balso atpažinimo programinės įrangos ir garso įrašymo technologijos pažangumo, įrašomo pokalbio garsumo[278].

Taigi nustatyti vieną visiems bepiločiams orlaiviams taikomą, privatumą apsaugantį atstumą neįmanoma, nes atstumas, iš kurio gali būti užfiksuoti geros kokybės vaizdai ir garsas priklauso nuo bepiločio orlaivio konfigūracijos bei kitų kintamųjų, tokių kaip vaizdo kameros, garso aparatūra, veido atpažinimo ir balso atpažinimo programinė įranga, aplinkos, kurioje vykdomas skrydis, veiksniai. Atitinkamai ir pirmoji reguliavimo kryptis privatumui apsaugoti yra nepakankama, dėl nuolatinių technologinių bepiločių orlaivių, veido atpažinimo ir garso atpažinimo programinės įrangos pokyčių toks reglamentavimas arba jau pasenęs, arba greitai pasens.

Taigi, dabartinis specialusis bepiločių orlaivių reguliavimas, kai reikalaujama laikytis konkretaus horizontalaus atstumo, yra labiau skirtas apsaugoti žmonių sveikatą ar gyvybę, jeigu bepilotis orlaivis netikėtai nukristų skrydžio metu, o ne užtikrinti trečiųjų asmenų privatumą. Šaltiniuose numatyti konkretūs atstumai (pvz., 15 m arba 30 m[279]) gali būti trumpalaikė ir netiesioginė privatumo apsaugos priemonė nuo tokių bepiločių orlaivių, kurių vaizdo kamera nepasižymi labai aukšta raiška, o mikrofonai geromis garso įrašymo galimybėmis. Visgi kiekvienos individualios situacijos vertinimas siekiant tiksliai nustatyti, ar tam tikras atstumas apsaugotų asmenų privatumą nuo bepiločių orlaivių, reikalautų per didelių laiko sąnaudų. Todėl tokia priemonė nebūtų veiksminga saugantis nuo grėsmių, kylančių privatumui dėl bepiločių orlaivių naudojimo.

2.3.2. Reikalavimas informuoti (arba gauti sutikimą)

Kitas netiesioginis privatumo apsaugos būdas yra reikalavimas informuoti arba gauti sutikimą. Jeigu bepiločio orlaivio valdytojas turėtų veiksmingą būdą informuoti asmenis, kad bus vykdomas skrydis ir renkami jų duomenys, o šie galėtų įvertinti, ar skrydis kels grėsmę jų privatumui, ir paprastu būdu duoti savo sutikimą, tuomet jų privatumas turėtų būti apsaugotas. Asmuo

278 Žr. Oliver Jokisch ir kt., „Audio and Video Processing of UAV-Based Signals in the Harmonic Project“, *Studientexte zur Sprachkommunikation: Elektronische Sprachsignalverarbeitung* 2021, (2021), 77–86; Kheireddine Choutri ir kt., „A Multi-Lingual Speech Recognition-Based Framework to Human-Drone Interaction“, Electronics 11, 12 (2022): 1829, https://doi.org/10.3390/electronics11121829.

279 ICAO dokumentai numato bendrą pareigą laikytis 30 m horizontalaus atstumo, jei negautas pašalinio asmens sutikimas. Jei sutikimas nėra gautas, tuomet – 15 m atstumo. Pareigą laikytis 30 m horizontalaus atstumo numato ir ES, jeigu skrydis vykdomas bepiločiu orlaiviu, kurio svoris didesnis kaip 900 g.

suprasdamas, kokiems tikslams ir kokie duomenys bus naudojami, gali nuspręsti, ar toje situacijoje privatumo apsauga jam yra būtina. Vis dėlto informavimo (sutikimo) pareiga gali būti problemiška. Pirma, ar dabartinis reguliavimas numato veiksmingą informavimo būdą, kuris užtikrintų, jog pašaliniai asmenys būtų tinkamai informuoti. Antra, taip pat nėra aišku, ar dabartinis reguliavimas užtikrina veiksmingą būdą aplinkiniams duoti sutikimą. Vertėtų panagrinėti, kaip šį reikalavimą įtvirtina skirtingos organizacijos. Reikalavimą informuoti (gauti sutikimą) numato ICAO, ES ir JAV reguliavimas, o JARUS rekomendacijose to nėra.

ICAO pavyzdiniai reglamentai nurodo, kad bepilotį orlaivį pilotuojantis asmuo norėdamas vykdyti skrydį virš ir arčiau kaip 30 m atstumu (matuojant horizontaliai) nuo asmens ar privataus žemės sklypo privalo gauti individo arba žemės sklypo savininko (naudotojo) sutikimą[280]. Ši nuostata reiškia, kad gauti sutikimą būtina tiktai tuo atveju, jeigu skrydis vykdomas arčiau kaip 30 m atstumu nuo pašalinio asmens (ar privataus žemės sklypo) arba virš jų, tačiau tais atvejais, kai skrydis vykdomas iš toliau ir ne tiesiai virš pašalinių asmenų ar objektų, sutikimo gauti nebūtina. Sutikimas taip pat neprivalomas, jeigu bepiločio orlaivio pilotas prieš skrydį gavo nacionalinės aviacijos organizacijos leidimą arba vykdo skrydį oro erdvėje, kurią minėta organizacija valdo[281]. ICAO siekia šių tikslų: 1) informuoti pašalinius asmenis apie vykdomą skrydį, kad šie galėtų reaguoti į pateiktą pranešimą, 2) ši taisyklė skatina keistis informacija apie pavojus, susijusius su skrydžiu arba numatomo skrydžio vietoje, 3) asmenys, kuriems skrydis daro įtaką, gali pasišalinti iš numatomos skrydžio teritorijos arba joje likti, atsižvelgdami į kylančias rizikas.

Nors ICAO savo dokumentais aiškiai planavo neapimti privatumo aspektų, tačiau apie informavimo (sutikimo) nuostatą yra pasisakę viename savo patariamųjų aplinkraščių, tikriausiai pastebėję šios taisyklės galimą sąsają su privatumo apsauga. ICAO pažymi, jog sutikimo taisyklė nėra skirta spręsti galimus privatumo pažeidimo klausimus, kylančius dėl bepiločių orlaivių skrydžių, todėl ir pilotai neturėtų manyti, kad gavę sutikimą jie atleidžiami nuo kitų nacionalinių valdžios institucijų privatumo apsaugos reikalavimų[282]. Iš šio komentaro galima suprasti, kad ICAO reikalavimą gauti sutikimą traktuoja kaip vieną iš būdų apsaugoti privatumą, tačiau abejoja, kad vien ji galėtų išspręsti visas su privatumo apsauga susijusias problemas, t. y. pareiga gauti sutikimą turėtų būti derinama su kitais privatumo nacionaliniais teisės aktais. Dar vertėtų išsiaiškinti, ar apskritai ICAO informavimo (sutikimo) nuostata netgi kartu su kitomis privatumo apsaugos priemonėmis galėtų užtikrinti kokią nors privatumo apsaugą.

Pagal ICAO taisyklę pašaliniai asmenys turi teisę į visą 30 m spindulio (matuojant horizontaliai) oro erdvės stulpą nuo žemės paviršiaus,

280 *ICAO model UAS regulations* part 101 and 102, *supra note,* 22, 101.25 straipsnis, a dalis, 1 punktas, i pastraipa,13.

281 *Ibid.,* b dalis, 13.

282 *ICAO Advisory Circular (AC) 101-1, supra note,* 22: 11.

o žemės sklypų savininkai turėtų turėti teisę į oro erdvės stulpą, esantį tiesiai virš žemės sklypo, ir taip pat 30 m spinduliu (matuojant horizontaliai) nuo žemės sklypo ribos. Iki kokio aukščio turėtų tęstis oro erdvės stulpas, to ICAO reguliavimas neapibrėžia. Pilotas norėdamas bepiločiu orlaiviu įskristi į pašalinių asmenų oro erdvę turėtų gauti jų sutikimą, t. y. juos informuoti apie planuojamą vykdyti skrydį. Praktiškai bepiločio orlaivio pilotui gali būti itin sudėtinga nustatyti, ar nepateks į kieno nors kito oro erdvę mažesniu nei 30 m atstumu, dėl ko jam reikėtų prašyti visų skrydžio teritorijoje esančių asmenų sutikimo.

ICAO siūlomą sutikimo procedūrą būtų sunku įgyvendinti, jeigu pačiam sutikimui nebūtų keliami tokie nedideli reikalavimai. Patariamajame aplinkraštyje, komentuojančiame pavyzdinio reglamento reikalavimus, nurodoma, jog sutikimas gali būti įvairių formų, t. y. ne tik aiškus, oficialus ar neoficialus, bet ir numanomas[283]. Kokie pašalinių asmenų veiksmai lemtų numanomą sutikimą, labai priklauso nuo faktinių aplinkybių, nacionalinių teisės aktų, nacionalinės teismų praktikos, tačiau vien šios sutikimo formos numatymas reglamentavime suteikia galimybę bepiločių orlaivių valdytojams piktnaudžiauti. Neišvengiamai kiltų klausimų, kuriuos pajėgūs išspręsti tik teismai, tarp jų, pvz.: jeigu asmuo vizualiai mato bepilotį orlaivį ir jo nuotolinį pilotą, tačiau pilotui neišreiškia pretenzijos dėl vykdomo skrydžio, ar galima sakyti, kad toks asmuo davė numanomą sutikimą vykdyti skrydį? Arba kitas pavyzdys, jeigu prie įvažiavimo į miestą nurodoma, jog miestas stebimas bepiločiais orlaiviais, ir asmuo savanoriškai vis tiek įvažiuoja į miestą, tai gali būti laikoma asmens numanomu sutikimu būti stebimam bepiločiais orlaiviais? Kita vertus, gauti kitokios formos (aiškų, oficialų ar neoficialų) sutikimą bepiločio orlaivio valdytojui gali būti labai sudėtinga, todėl tokia nuostata būtų praktiškai neįgyvendinama.

ICAO reguliavimas numato ir atvejį, kada sutikimas neprivalomas, t. y. kai gautas nacionalinės aviacijos organizacijos leidimas. Jeigu leidimą išduodanti institucija atliktų ne tik skrydžio saugos, bet ir privatumo rizikos vertinimus, kiekvienas skrydžio, kuriam reikalingas leidimas, atvejis būtų labai individualizuojamas, todėl į galimas grėsmes privatumui būtų atsižvelgiama labiau. Vis dėlto privatumo apsaugos veiksmingumas labai priklauso nuo nacionalinių įgyvendinamųjų teisės aktų, kurie nustatytų leidimų išdavimo tvarką bei privatumo rizikos vertinimo procedūras. Tinkamai suformuluoti teisės aktai galėtų reikšti veiksmingą privatumo apsaugą, tačiau biurokratiškai išdėstyti poįstatyminiai teisės aktai galėtų lemti visiškai neveikiančią sistemą. Taigi teoriškai leidimo išdavimo procedūra galėtų užtikrinti pakankamą privatumo apsaugą, tačiau tik tuo atveju, jeigu nacionaliniu mastu galiotų tinkamai suformuluoti teisės aktai.

ES dokumentai numato pareigą informuoti (gauti sutikimą) iš pašalinių asmenų, kai vykdomas atvirosios kategorijos (A2 ir A3 pakategorės) skrydis bepiločiu orlaiviu, kurio svoris didesnis kaip 900 g[284]. Jeigu bepiločio orlaivio svoris

283 *ICAO Advisory Circular (AC) 101-1, supra note,* 22: 11.

284 Reglamento (ES) 2019/947 priedo A dalies „UAS.OPEN.050. UAS naudotojo pareigos“ skyriaus 7 punktas.

mažesnis negu 900 g, specialieji ES bepiločių orlaivių reglamentai nenumato pareigos informuoti ar gauti sutikimą. Vykdant komercinius specialiosios kategorijos skrydžius, t. y. tokius, kuriems reikia atskiro nacionalinės aviacijos organizacijos leidimo (kai gabenami pavojingi kroviniai, BVLOS ar visiškai autonominis skrydis), nepriklausomai nuo bepiločio orlaivio svorio, bepiločio orlaivio naudotojas privalo turėti patvirtintas asmens duomenų tvarkymo taisykles, kuriose būtų numatytos asmens duomenų tvarkymo procedūros pagal BDAR[285], t. y. vykdydamas tokį skrydį bepiločio orlaivio valdytojas privalo vadovautis BDAR. Vienas iš BDAR 6 straipsnyje numatytų teisinių pagrindų tvarkyti asmens duomenis (tarp jų ir, pvz., asmens atvaizdą užfiksuotą bepiločio orlaivio vaizdo kamera) yra sutikimas[286].

Nors iš Reglamento (ES) 2019/947 galima susidaryti įspūdį, kad informavimo (sutikimo) pareiga pagal BDAR reikalavimus saisto tik specialiosios kategorijos skrydžius vykdančius bepiločių orlaivių valdytojus, o prieš vykdant atvirosios kategorijos skrydžius pašalinių asmenų sutikimą gauti privaloma tiktai Reglamente (ES) 2019/947 numatytais atvejais (t. y. bepiločio orlaivio svoriui viršijus 900 g), tačiau atidžiau panagrinėjus BDAR ir ESTT jurisprudenciją, vaizdas tampa painesnis. BDAR netaikomas tada, kai duomenis tvarko fizinis asmuo, užsiimantis išimtinai asmenine ar namų ūkio veikla[287], vadinasi, BDAR neturėtų būti taikomas daugeliui atvirosios kategorijos bepiločių orlaivių skrydžių, kuriuos vykdo fiziniai asmenys. Vis dėlto ESTT praktika, susijusi su CCTV kamerų naudojimu, numato, kad „asmeninės ar namų ūkio veiklos išimtis“ netaikoma, kai asmens duomenys renkami viešosiose erdvėse[288]. Nors ši praktika nėra tiesiogiai susijusi su bepiločiais orlaiviais, tačiau tikėtina, jog vadovaujantis ja bet kokiems viešoje vietoje vykdomiems skrydžiams būtų taikomi BDAR reikalavimai. Vadinasi, nepriklausomai nuo bepiločio orlaivio svorio, BDAR reikalavimai, tarp jų ir informavimo (sutikimo) taisyklės, pagal ES teisę būtų taikomos visiems bepiločių orlaivių skrydžiams, kurie vykdomi viešoje vietoje. Tačiau tai nereiškia, kad visiems skrydžiams bepiločiu orlaiviu būtina gauti sutikimą.

Vertinant šias nuostatas sistemiškai, reikėtų suprasti, kad vykdant skrydžius bepiločiu orlaiviu, kurio svoris didesnis kaip 900 g, pašalinių asmenų sutikimą gauti reikia visuomet, nebent bepiločio valdytojas turi nacionalinės aviacijos organizacijos leidimą. Skrydžiams bepiločiu orlaiviu, kurio svoris mažesnis kaip 900 g, pašalinių asmenų sutikimo nereikia, jeigu skrydis vykdomas privačioje erdvėje. Jeigu skrydis lengvesniu kaip 900 g bepiločiu orlaiviu vykdomas viešoje vietoje, sutikimą pagal BDAR gauti būtina, jeigu nėra kitų BDAR 6 straipsnyje numatytų duomenų tvarkymo pagrindų. Jeigu skrydis vykdomas kitais BDAR 6 straipsnyje

285 Reglamento (ES) 2019/947 priedo B dalies „UAS.SPEC.050. UAS naudotojo pareigos“ skyriaus 1 punktas, a dalis, iv punktas, BDAR.

286 BDAR, 6 straipsnio 1 dalies a punktas.

287 BDAR, preambulės 18 punktas, 2 straipsnio 2 dalies c punktas.

288 Žr. „Case C-212/13 on CCTV“. http://curia.europa.eu/juris/document/document.jsf?text=95%252F46%252FEC&docid=160561&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=300923#ctx1.

numatytais pagrindais, tuomet vykdant skrydį mažesniu kaip 900 g bepiločiu orlaiviu sutikimo gauti nereikia. BDAR numatyti pagrindai yra šie: 1) kai tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu, prieš sudarant sutartį[289], 2) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė[290], 3) tvarkyti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus[291], 4) tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas[292] arba 5) tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų[293]. Šiame poskyryje apsiribosime reikalavimu informuoti (gauti sutikimą).

Detali BDAR reikalavimų sutikimui analizė atliekama disertacijos 4.2.1 poskyryje, todėl čia toliau nebus plėtojama. Trumpai tariant, norint skrydį vykdyti šiuo BDAR pagrindu, sutikimą reikėtų gauti visuomet. Pagrindinis šios priemonės trūkumas yra tas, jog sutikimą ne visada lengva gauti. Sudėtingiausia sutikimus būtų gauti viešoje vietoje skrydžius vykdantiems vidutiniams vartotojams. Jie, tikėtina, šios normos tiesiog nepaisytų. Dėl to gali kilti saugumo neužtikrinimo ir atidengimo pažeidimų. Sutikimą taip pat būtų sudėtinga gauti, jeigu skrydžio tikslas *a priori* yra tvarkyti asmens duomenis (pvz., stebėti konkrečius asmenis, žmonių minią ar teritoriją, fiksuoti mobiliųjų telefonų duomenų ryšį ir pan.), todėl tokiu atveju duomenis rinkti skrydžio metu duomenų tvarkytojas tikriausiai vykdytų kitais BDAR 6 straipsnyje numatytais pagrindais. Išimtys galimos nebent tada, jeigu bepiločiu orlaiviu vieša vieta tik filmuojama, o duomenys arba neįrašomi į laikmeną, arba dar iki jų įrašymo į laikmeną būna visiškai anonimizuojami (žr. disertacijos 4.2.1 poskyrį).

JAV federalinių teisės aktų kodekso 107 dalis nenumato reikalavimo informuoti pašalinius asmenis apie planuojamą skrydį ar gauti jų sutikimą, bet laikytis informavimo (sutikimo) praktikos rekomenduojama Gerosios praktikos gairėse[294]. Kalbant apie informavimo pareigą, gairės numato, jog bepiločio orlaivio valdytojas turėtų pasistengti iš anksto pranešti asmenims, kada ir kurioje vietoje bepiločiu orlaiviu planuojama rinkti asmens duomenis. Pvz., bepiločių orlaivių valdytojai klientams gali pateikti numatomą jų prekių pristatymo laiką, o nekilnojamojo turto specialistai, naudojantys bepiločius orlaivius, gali iš anksto pranešti namo pardavėjui (ir galbūt artimiausiems kaimynams) apie numatomą jų turto fotografavimo datą. Kai skrydį planuojama vykdyti mėgėjiškais tikslais, pranešimas netoli esantiems

289 BDAR, 6 straipsnio 1 dalies b punktas.
290 *Ibid.,* c punktas.
291 *Ibid.,* d punktas.
292 *Ibid.,* e punktas.
293 *Ibid.,* f punktas.
294 Voluntary Best Practices for UAS Privacy, Transparency, and Accountability, *supra note,* 263.

asmenims nebūtinas[295]. Gerosios praktikos gairėse bepiločių orlaivių valdytojams, planuojantiems rinkti asmens duomenis, taip pat rekomenduojama turėti viešai prieinamą privatumo politiką, kurioje būtų nurodyti planuojamų rinkti duomenų tipai, duomenų rinkimo tikslai, duomenų saugojimo ir nuasmeninimo praktikos, subjektų, kuriems bus prieinami surinkti duomenų pavyzdžiai, informacija, kaip pateikti skundus dėl privatumo ar duomenų apsaugos klausimų, informacija, apibūdinanti reagavimo į teisėsaugos prašymus praktiką[296]. Gairėse numatyta, kad bepiločio orlaivio valdytojas sutikimą privalo gauti tuomet, jeigu žino, kad duomenų subjektas pagrįstai gali tikėtis privatumo, taip pat jeigu vykdo skrydį virš privačios nuosavybės objektų arba privačios nuosavybės objektų viduje[297].

Daug diskutuoti, kaip JAV specialusis bepiločių orlaivių reguliavimas aptaria informavimo (sutikimo) procedūrą nėra prasmės, nes informuoti aplinkinius ir tam tikrais atvejais gauti jų sutikimą yra tiktai rekomenduojama, bet neprivaloma. Kita vertus, standartizavimo sprendimais, galbūt, pasirinktas kitoks, mažiau intervensinis kelias, negu tas, kuriuo eina ICAO ir ES, kai privatumo dilemos, susijusios su bepiločių orlaivių naudojimu, paliekamos spręsti teismams. Gerosios praktikos gairės bent šiuo metu tai palieka spręsti bepiločių orlaivių valdytojams: būtų įsibraunama į kieno nors asmeninę erdvę ar ne, reikia pašalinius asmenis informuoti ir gauti jų sutikimą ar ne. Tokia sistema palanki bepiločių orlaivių valdytojams, tačiau jos veiksmingumas privatumui apsaugoti – abejotinas.

Kiekvienoje analizuojamoje jurisdikcijoje reikalavimas informuoti (gauti sutikimą) įgyvendinamas kiek skirtingai. ICAO sutikimo reikalingumą sieja su atstumu, kuriuo bepiločiu orlaiviu planuojama skristi nuo pašalinių asmenų, ES taisyklės šį reikalavimą sieja su bepiločio orlaivio mase ir vieta, kurioje vykdomas skrydis, JAV standartizuojantys reguliavimo šaltiniai laikosi labiau ad hoc požiūrio. Įvertinus visų analizuotų jurisdikcijų taisykles matyti, kad informavimo (sutikimo gavimo) reikalavimai nebūtų veiksmingas būdas apsaugoti privatumą. Tokia išvada daroma dėl informavimo (sutikimo gavimo) sudėtingumo. Skrydžiai bepiločiais orlaiviais reikšmingai skiriasi nuo naršymo internete. Internetinėje erdvėje sutikimo galima paprašyti prieš asmeniui pradedant naudotis tinklalapiu, o šiam nesutikus, tinklalapis gali automatiškai išsijungti arba tiesiog nerinkti duomenų apie lankytoją. Realiame pasaulyje sunku įsivaizduoti mechanizmą, kuris visus bepiločio orlaivio skrydžio teritorijoje esančius žmones automatiškai informuotų apie planuojamą skrydį, o jei šie nesutiktų, duomenų apie juos nerinktų. Matyt, dėl to ICAO reikalavimas minimalus – t. y. sutikimas gali būti numanomas, tačiau vien šios sutikimo formos numatymas reglamentavime sudaro galimybę bepiločių orlaivių valdytojams piktnaudžiauti. ES reikalavimai sutikimui labai griežti ir išsamūs, bet praktiškai neįgyvendinami vykdant skrydžius ten, kur yra didesni žmonių susibūrimai. JAV laikomasi požiūrio, kad šiuo metu nustatyti reikalavimą

295 *Ibid.,* 5.
296 *Ibid.*
297 *Ibid.,* 6.

informuoti ir gauti aplinkinių sutikimą nėra būtina, todėl šios pareigos laikytis tik rekomenduoja ir tik tuomet, kai pats bepiločio orlaivio valdytojas mano, kad gali pažeisti kažkieno asmeninę erdvę.

2.3.3. Registracijos reikalavimas

Dar vienas būdas, kuriuo dabartinis bepiločių orlaivių reguliavimas gali prisidėti prie privatumo apsaugos, yra registracijos reikalavimas. ICAO pavyzdinio reglamento 101.5 straipsnis numato, kad bet kas, valdantis ir planuojantis skraidinti bepilotį orlaivį, privalo jį atitinkamoje valstybėje įregistruoti ir turėti galiojantį registravimo sertifikatą. JARUS rekomendacijos numato tokį patį reikalavimą, tik nustato, kad išimtis turėtų būti padaryta bepiločiams orlaiviams, kurių svoris neviršija 250 g (A1 pakategorė)[298].

Reglamento (ES) 2019/947 14 straipsnio 1 dalis numato valstybių narių pareigą registruoti bepiločių orlaivių naudotojus, kurių veikla gali kelti riziką saugai, saugumui, privatumui, asmens duomenų apsaugai ar aplinkai. Reikalavimas registruotis taikomas visų bepiločių orlaivių valdytojams neatsižvelgiant į kategoriją, nebent jų valdomas bepilotis orlaivis sveria mažiau kaip 250 g ir prie jo nepritaisyti jutikliai, kuriais galima būtų fiksuoti asmens duomenis. Registruotis pagal ES reglamentavimą neprivaloma ir žaislinių bepiločių orlaivių, atitinkančių Direktyvos 2009/48/EB reikalavimus, kai jų svoris nesiekia 250 g, valdytojams. Papildomas reikalavimas registruoti ne tik bepiločio orlaivio valdytoją, bet ir patį bepilotį orlaivį yra numatytas tada, kai skrydis vykdomas sertifikuotos klasės bepiločiu orlaiviu[299].

JAV registruoti bepiločius orlaivius privaloma visiems skrydžius vykdantiems privatiems valdytojams. Bendra tvarka skrydžius vykdantys asmenys privalo registruoti savo bepiločius orlaivius pagal CFR 14 antraštės 48.15 straipsnį[300], rekreacinius – pagal rekreacinių skrydžių išimtį, numatytą USC 49 antraštės 44809 straipsnyje[301].

Nors visos analizuojamos jurisdikcijos turi reikalavimą bepiločius orlaivius arba valdytojus registruoti, bet tarp jų yra skirtumų. Pvz., ICAO ir JAV numato, kad registruoti privaloma visus bepiločius orlaivius be išimties. JARUS ir ES taiko tam tikras išlygas. JARUS daro išimtį bepiločiams orlaiviams, kurių svoris nesiekia 250 g, nepriklausomai nuo to, kokiais tikslais vykdomas skrydis. ES išsiskiria iš kitų jurisdikcijų, nes nenumato bendros pareigos registruoti bepiločius orlaivius. Tačiau ES numato pareigą registruotis jų valdytojams, o pačius bepiločius orlaivius

298 „JARUS Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, *supra note,* 273, 5 straipsnio 1 dalis, skyrius „UAS.OPA.30 Registration of UA“.

299 Reglamento (ES) 2019/947 14 straipsnis.

300 14 United States Code of Federal Regulations 48.15(b).

301 49 United States Code 44809: Exception for limited recreational operations of unmanned aircraft.

registruoti reikalauja tik tuomet, jeigu vykdomi specialiosios kategorijos skrydžiai. Išimtys, kada bepiločių orlaivių valdytojams galima nesiregistruoti, ES taip pat išskirtinės, t. y. kai: 1) bepilotis orlaivis negali fiksuoti asmens duomenų (neturi tam reikalingų jutiklių, pvz., filmavimo kameros) ir sveria mažiau kaip 250 g; 2) yra laikomas žaislu pagal Direktyvą 2009/48/EB ir sveria mažiau kaip 250 g (net jeigu žaislinis bepilotis orlaivis turi kamerą ar kitus jutiklius[302]).

Apskritai kalbant apie registravimo reikalavimą, pažymėtina, jog registracija turėtų prisidėti prie privatumo apsaugos, nes valdytojas vien žinodamas, kad jo bepilotis orlaivis arba jis pats yra registruotas kaip vykdantis skrydžius, psichologiškai turėtų jaustis labiau įpareigotas elgtis pavyzdingai. Panašų visuomenės požiūrį atskleidė ir 2017 m. JAV atlikta apklausa[303], visgi dauguma apklausoje dalyvavusių respondentų abejojo, jog registracijos reikalavimas galėtų tiesiogiai prisidėti prie žmonių privatumo apsaugos[304]. Ši abejonė kyla dėl to, kad registracija tik užtikrina, jog prasižengę valdytojai neliktų nenubausti, bet tiesiogiai pažeidimams kelio neužkerta. Vis dėlto tinkamai įgyvendintas reikalavimas registruotis būtų puikus netiesioginis būdas privatumui apsaugoti, nes gali užtikrinti teisę kreiptis į teismą dėl teisminės gynybos[305].

Registracijos svarbą galėtų iliustruoti paprastas atidengimo pažeidimo pavyzdys. Tarkim, asmuo laisvalaikiu deginasi jam nuosavybės teise priklausančiame žemės sklype ir pastebi, jog netoli jo sklypo ribos kybo nedidelis bepilotis orlaivis. Taigi asmuo norėtų sužinoti: ar bepiločiu orlaiviu nebuvo užfiksuota jautri, su jo privačiu gyvenimu susijusi informacija, taip pat ar ši nebus paskleista viešai be jo sutikimo.

Pavyks asmeniui apginti savo pažeistą teisę į privatumą ar ne, pirmiausia priklauso nuo to, ar jis galės identifikuoti pažeidėją. Registracija, nors ir nebūtinai užtikrina galimybę nustatyti pažeidėjo tapatybę, nes nukentėjusysis turėtų kažkaip sužinoti bepiločio orlaivio identifikavimo numerį registre, vis dėlto yra pirmas žingsnis identifikuojant. Tai, kad bepilotis orlaivis siejamas su konkrečiu asmeniu, teikia realią galimybę pažeidėją identifikuoti, tik reikia rasti būdų, kaip sužinoti

---

302 EASA savo tinklalapyje nurodo, kad „registruotis bepiločio orlaivio valdytojui nereikia, jeigu: 1) bepilotis orlaivis sveria mažiau nei 250 g ir neturi kameros ar kito jutiklio, gebančio fiksuoti asmens duomenis; 2) Net ir su kamera ar kitu jutikliu sveria mažiau nei 250 g, tačiau yra žaislas (tai reiškia, kad jo dokumentacija rodo, kad jis atitinka Direktyvą 2009/48/EB)“ (aut. vert.), žr. „Civil Drones (Unmanned Aircraft)“, EASA, žiūrėta 2020 m. rugsėjo 14 d., https://www.easa.europa.eu/domains/civil-drones-rpas.

303 Tyrimo apibendrinimas: „nors nė vienas mechanizmas nebuvo suvokiamas kaip „sidabrinė kulka“, savininkų registracija ir veidų suliejimas įgijo palyginti daugiau pašalinių asmenų ir dronų valdytojų palaikymo nei kiti mechanizmai“ (aut. vert.), žr. Yaxing Yao ir kt., „Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders“, *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (ACM, 2017), 6785.

304 *Ibid.,* 6782.

305 Europos mastu ši teisė įtvirtina EŽTK 6 straipsnio 1 dalyje, Lietuvoje šią teisę įtvirtina LR Konstitucijos 30 straipsnio 1 dalis.

jo teises pažeidusio bepiločio orlaivio identifikavimo numerį[306]. Tačiau jeigu bepiločiai orlaiviai nebūtų paženklinti unikaliu numeriu, kuris susietas su informacija galimybė pažeidėją identifikuoti ir paduoti jį į teismą, gali būti neįgyvendinama. Pateiktame pavyzdyje išpuolio auka netgi fiziškai matydama, kas yra bepiločio orlaivio valdytojas (pvz., jeigu jis yra netoli valdomo bepiločio orlaivio), negalėtų jo paduoti į teismą, jeigu nežinotų jo asmens duomenų, tokių kaip vardas, pavardė, asmens kodas, adresas[307]. Kad asmuo duomenis sužinotų, jis turėtų apie incidentą pranešti policijai, kuri pažeidėją galėtų rasti pagal nukentėjusiojo pasakojimus (veido bruožus, aprangą, bepiločio orlaivio modelį ir pan.), bet tokiu būdu ginti teises pernelyg sudėtinga, nei pažeidėjo tapatybę nustatyti pagal unikalų valdytojo ar bepiločio orlaivio numerį. EŽTT yra pasisakęs, kad teisė kreiptis į teismą turi būti „praktiška ir veiksminga“[308]. Tam, kad teisė kreiptis į teismą būtų veiksminga, asmuo turi „turėti aiškią, praktišką galimybę užginčyti veiksmą, kuris yra kišimasis į jo teises“[309]. Nukentėjusysis, negalėdamas identifikuoti pažeidėjo, susiduria su labai rimta procedūrine kliūtimi, kuri neleidžia praktiškai ir veiksmingai ginti savo teisių. Tad registracijos reikalavimas būtų viena svarbiausių privatumo apsaugos priemonių, didinančių žmonių galimybes turėti teisminę gynybą.

Tiesa, yra ir tų, kurie mano, jog registracijos reikalavimas gali pažeisti bepiločių orlaivių valdytojų privatumą[310]. Bepiločių orlaivių ar jų valdytojų registrai paprastai nėra vieši, jie prieinami tik valdžios institucijoms, todėl grėsmė privatumui galėtų kilti, jei valstybės institucijos piktnaudžiautų surinkta informacija ar nepakankamai užtikrintų jos saugumą. Grėsmės, kurios gali kilti padidinus valstybei prieinamą informacijos kiekį, jau buvo aptartos ankstesniame disertacijos skyriuje nagrinėjant *identifikavimo* ir *saugumo* neužtikrinimo pažeidimus. Taigi registracijos reikalavimas teoriškai galėtų pažeisti bepiločių orlaivių valdytojų privatumą.

---

306 Galimybę identifikuoti bepilotį orlaivį ar jo valdytoją gali suteikti nuotolinio identifikavimo priedai, apie tai plačiau disertacijos 2.3.7 poskyryje „Nuotolinio identifikavimo priedai“.

307 Pvz., LR civilinio proceso kodekso 111 straipsnis numato bendruosius reikalavimus teismui teikiamiems procesiniams dokumentams, teismui, *inter alia,* būtina pateikti dalyvaujančių byloje asmenų procesines padėtis, vardus, pavardes, asmens kodus (jeigu jie žinomi), gyvenamąsias vietas.

308 „Bellet v. France“, 4 December 1995, Series A no. 333-B, 38 pastraipa, „Zubac v. Croatia [GC]“, no. 40160/12, 5 April 2018, 76–79 pastraipos.

309 „Bellet v. France“, *Ibid.,* 36 pastraipa, „Nunes Dias v. Portugal“ (dec.), nos. 2672/03 and 69829/01, ECHR 2003-IV, „Fazliyski v. Bulgaria“, no. 40908/05, 16 April 2013.

310 Visuomenės atliktoje apklausoje dalis bepiločių valdytojų (5 proc.) buvo susirūpinę, kas gali pasiekti jų registracijos informaciją, ir paminėjo, kad tik vyriausybė gali naudotis ta informacija. Kai kurie valdytojai pastebėjo, kad dėl šio mechanizmo gali didėti vyriausybės galimybės sekti jų veiklą. Vienas valdytojas taip apibendrino: „Manau, kad tai geras ir blogas dalykas. Geras tuo, kad jei kas nors naudoja bepilotį orlaivį neteisėtai veiklai, būtų lengva nustatyti jo bepiločio orlaivio informaciją, jei apie tai būtų pranešta. Blogas, nes tai dar vienas būdas vyriausybei stebėti žmonių veiklą.“ (Aut. vert.), žr. Yao ir kt., „Privacy Mechanisms for Drones“, *supra note,* 307.

Visgi grėsmės, kylančios privatumui, lygis labai priklauso nuo valstybės kaupiamos informacijos pobūdžio. ICAO ir JARUS savo rekomendacijose konkrečiai nenurodo, kokią informaciją valstybės turėtų kaupti bepiločių orlaivių registruose. JAV bepiločių valdytojus reikalauja pateikti el. pašto adresą, fizinį pašto adresą, bepiločio orlaivio gamintoją, modelį, serijinį numerį. Jeigu registracija vykdoma elektroniniu būdu, pareiškėjai, mokėdami registracijos mokestį, papildomai privalo nurodyti kreditinės ar debetinės kortelės informaciją (t. y. kreditinės kortelės numerį, galiojimo datą, saugos kodą ir atsiskaitymo adresą)[311]. ES teisės aktai numato, jog registracijos sistemoje turi būti įrašyta skrydį vykdančio fizinio asmens vardas ir pavardė, gimimo data arba juridinio asmens pavadinimas ir kodas, kontaktiniai duomenys, turimi leidimai)[312].

Analizuojamų jurisdikcijų teisinis reguliavimas, numatantis bepiločių orlaivių (jų valdytojų) registre kaupti duomenis, nėra pernelyg jautrūs, nes valstybės juos ir taip kaupia, kad būtų užtikrintas kasdienių administracinių operacijų sklandumas. Didesnis pavojus bepiločių valdytojų privatumui galėtų kilti, jeigu valstybės kauptų ne tik pagrindinius asmens duomenis, bet ir, pvz., duomenis apie bepiločio orlaivio lokaciją, realiu laiku formuotų metaduomenis apie bepiločio orlaivio aplinką, skrydžio tikslus ir pan., tačiau kol tokios informacijos valstybės nekaupia. Registracijos nauda pašaliniams asmenims nusveria privatumo grėsmes, kurios kiltų bepiločių orlaivių valdytojams įvedus tokį reikalavimą.

Taigi teoriškai registracijos reikalavimas yra gera privatumo apsaugos priemonė, bet praktiškai jos veiksmingumas priklauso nuo įgyvendinimo. Kitaip tariant, net ir gerą privatumo apsaugos priemonę gali sugadinti biurokratiškas reglamentavimas, kuris sudarytų dirbtinių kliūčių ją įgyvendinti. Todėl vertėtų padiskutuoti, ar analizuojamų jurisdikcijų siūlomi registracijos reguliavimo variantai būtų pakankami ir ar kuris nors iš būdų reglamentuoti registraciją yra geresnis už kitus.

Akivaizdus skirtumas tarp analizuojamų jurisdikcijų yra tas, kad vienos siūlo registruoti bepiločius orlaivius, o kitos – jų valdytojus. Disertacijos autoriaus nuomone, reikšmingo pranašumo nė vienas registracijos reguliavimo būdas neturi, nes ir vienu, ir kitu atveju bepilotis orlaivis būtų susietas su konkrečiu asmeniu, šito ir užtenka siekiant nustatyti pažeidimo kaltininką.

Kitas skirtumas – tai išimtys, kada registruotis nebūtina. JARUS reguliavimas numato, kad registracija nebūtina, kai bepiločio orlaivio svoris neviršija 250 g. ES bepiločio svoris ne tik turi neviršyti 250 g, bet ir negebėti fiksuoti asmens duomenų arba būti laikomas žaislu pagal Direktyvą 2009/48/EB, o ICAO ir JAV išimčių šiuo atžvilgiu iš viso nenumato. Registracijos išimtimis siekiama dviejų

311 „Aircraft Registration | Federal Aviation Administration“, žiūrėta 2022 m. gruodžio 16 d., https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/ua.

312 „Aircraft Registration | Federal Aviation Administration“, žiūrėta 2022 m. gruodžio 16 d., https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/ua.

tikslų: 1) neužkrauti per daug administracinės naštos valstybės institucijoms, 2) pernelyg nevarginti mėgėjų bepiločių orlaivių valdytojų administracinėmis procedūromis. Tačiau, darant įvairių kompromisų dėl valdžios institucijų ir nepatyrusių pilotų patogumo, neišvengiamai atsisakoma ir dalies apsaugos, kurią teikia registracijos reikalavimas.

Darant išimtis, kai atsižvelgiama vien į bepiločio orlaivio svorį, prasideda technologinės lenktynės tarp gamintojų, kurie siekia sukurti kuo pažangesnius lengvus bepiločius orlaivius su panašiomis asmens duomenų fiksavimo galimybėmis, kaip ir dideli, bet jiems pagal galiojančius teisės aktus registracija nebūtina. Pvz., viena žinomiausių bepiločių orlaivių gamintojų „DJI" išleido 249 g sveriantį „Mavic Mini", kuris suprojektuotas taip, kad neviršytų daugelio aviacijos organizacijų nustatyto 250 g. Tačiau „Mavic Mini", nors ir mažo svorio, turi konkurencingą kamerą, didžiulį veikimo diapazoną, labai įspūdingą skrydžio laiką ir daugelį vieno paspaudimo skrydžio režimų[313]. Tokia išimtis gamintojus tik skatina kurti ir naudoti lengvesnius, tačiau nebūtinai technologiškai paprastesnius bepiločius orlaivius. Jeigu „DJI" sugebėjo sukurti pažangiomis galimybėmis išsiskiriantį bepilotį orlaivį, kurio nereikia registruoti, netrukus, kai tik atsirado reguliavimas, numatantis svorio ribą, nuo kurios registracija privaloma. Taigi svorio išimtis yra neproporcingas kompromisas, kuris gerokai padidina grėsmę privatumui, o administracinę naštą sumažina nežymiai.

ICAO ir JAV nustatytas reikalavimas registruoti visus bepiločius orlaivius be išimties užtikrina maksimalią privatumo apsaugą, tačiau vartotojams ir valdžios institucijoms gali užkrauti papildomą naštą, nes registruojami ir žaisliniai bepiločiai orlaiviai, nekeliantys grėsmės privatumui.

Disertacijos autoriaus nuomone, reikalavimas registruoti visus bepiločius orlaivius be išimties pernelyg didelės administracinės naštos bepiločių orlaivių gamintojams nesukurtų, palyginti su nauda, kurią toks reikalavimas atneštų privatumo apsaugai. Šiuo atveju kompromisas prisidėtų prie privatumo apsaugos didinimo, taip pat nevaržytų bepiločių orlaivių technologijų tobulinimo, nebent apribotų nesudėtingų žaislinių bepiločių pardavimus.

ES daroma išimtis taip pat siejama su bepiločio orlaivio svoriu, tik numatant papildomų sąlygų. Viena jų – reikalavimas, kad bepilotis orlaivis negebėtų fiksuoti asmens duomenų, yra skirtas apsaugoti privatumą, kurį puikiai įgyvendina. Tuo tarpu reikalavimas, kad bepilotis orlaivis atitiktų Direktyvos 2009/48/EB reikalavimus, tikriausiai siejamas su technologiniu paprastumu, o tai gali kelti tam tikrų taikymo neaiškumų. Direktyvos 2009/48/EB, skirtos žaislų saugai, I priede pateiktas gaminių, kurie nėra laikomi žaislais, sąrašas, bet į jį bepiločiai orlaiviai neįtraukti, artimiausias jiems būtų 14 punktas, numatantis, jog žaislais negali būti laikoma: „elektroninė įranga, pvz., asmeniniai kompiuteriai ir žaidimų pultai,

313 Malek Murison, „DJI's Mavic mini is so small you don't have to register it with the FAA", *DRONELIFE* (blog), 2019 m. spalio 30 d., https://dronelife.com/2019/10/30/djis-new-mavic-mini-is-so-small-you-dont-have-to-register-it/.

reikalingi pasinaudoti interaktyvia programine įranga ir susijusius išorinius įrenginius, jeigu elektroninė įranga ar susiję išoriniai įrenginiai nėra specialiai suprojektuoti arba skirti vaikams ir patys savaime nėra žaislai, pvz., specialiai suprojektuoti asmeniniai kompiuteriai, klaviatūros, vairalazdės ar vairaračiai“[314]. Nors iš Direktyvos 2009/48/EB teksto nėra aišku, kokie bepiločiai orlaiviai būtų laikomi žaislais, tačiau abejotina, jog mažai sveriantys, sudėtingi bepiločiai orlaiviai, kurie nėra specialiai suprojektuoti vaikams (tarp jų, pvz., ir „Mavic Mini“), atitiktų reikalavimus, keliamus žaislams. Taigi išimtį siaurinančios sąlygos užtikrina, kad nė vienas privatumą galintis pažeisti bepilotis orlaivis ES neliktų neregistruotas, o kiti bepiločiai orlaiviai nesudarytų biurokratinių kliūčių ir būtų naudojami kaip žaislai.

Atlikus analizę nustatyta, kad registracijos reikalavimas – viena svarbiausių ir pirminių privatumo apsaugos priemonių, užtikrinančių asmenų galimybę įgyvendinti teisę kreiptis į teismą dėl gynybos, tačiau šį reikalavimą tinkamai įgyvendina ne visi specialieji bepiločių orlaivių reguliavimo šaltiniai. Išimtys, kurių taikymas priklauso vien nuo bepiločio orlaivio svorio (JARUS), gamintojams sudaro galimybes gaminti bepiločius orlaivius, kuriems nėra keliami griežtesni reikalavimai, bet privatumą jie gali pažeisti. Registruoti visus bepiločius (ICAO, JAV), nors yra geriau, nei numatyti tik svorio ribą, visgi tuomet gali būti ribojamas bepiločių orlaivių, kaip žaislų, naudojimas. Tad nuostatos (ES), kurios numato ne tik svorio ribą, bet ir papildomas sąlygas (bepilotis negali fiksuoti asmens duomenų arba yra žaislas), turėtų pasiteisinti ir galėtų būti gerosios praktikos pavyzdžiu kitų valstybių teisiniam reguliavimui.

2.3.4. Reikalavimas kaupti įrašus

Reikalavimas kaupti įrašus teoriškai galėtų būti netiesioginė privatumo apsaugos priemonė, kuri padėtų detaliau atkurti situaciją, kuomet įvykdytas tariamas pažeidimas. Tačiau nukentėjusiam asmeniui apginti savo teises gali padėti ne bet kokie duomenys, o tik tokie, kurie iškilus ginčui padėtų detaliau atkurti įvykio eigą. Taigi vertėtų detaliau panagrinėti, kaip šį reikalavimą traktuoja kiekviena iš analizuojamų jurisdikcijų ir ar jų privalomai kaupiami duomenys galėtų padėti apsaugoti privatumą. Pareigą kaupti įrašus numato ICAO, JARUS ir ES reguliavimas. Į JAV reguliavimą toks reikalavimas neįtrauktas.

ICAO pavyzdiniai reglamentai numato specialiosios kategorijos bepiločių orlaivių skrydžių valdytojų pareigą: 1) 12 mėnesių nuo sukūrimo datos kaupti kiekviename skrydyje dalyvaujančių nuotolinių pilotų ir kitų įgulos narių vardus bei pavardes, skrydžių laikus[315], 2) 24 mėnesius nuo sukūrimo datos kaupti įrašus,

---

314 „2009 m. birželio 18 d. Europos Parlamento ir Tarybos direktyva 2009/48/EB dėl žaislų saugos“, OJ L 170, 2009 m. birželio 30 d., 1–37, I priedo 14 punktas.

315 Taisyklė originalo kalba yra dviprasmiška: „A record containing the names of the remote pilots and other crew members involved in each flight, in respect of the system, **the time of each flight** or series of flights; and“. Frazė „the time of each flight“ gali reikšti tiek bepiločių orlaivių skrydžių valdytojų pareigą kaupti duomenis apie skrydžio laiką, tiek jų pareigą kaupti duomenis apie skrydžio trukmę.

kuriuose pateikiami sistemos techninės priežiūros veiksmai, modifikavimas ar remontas[316].

JARUS savo rekomendacijose numato, kad vykdydamas specialiosios kategorijos skrydžius bepiločio orlaivio valdytojas turėtų kaupti duomenis bent jau apie skrydžio trukmę ir su juo susijusią techninę priežiūrą, saugoti šią informaciją žurnalo (angl. *logbook*) ar lygiaverčio dokumento forma[317].

ES reglamentavimas numato, kad turintieji lengvųjų bepiločių orlaivių naudotojo pažymėjimą (LUC)[318] privalo ne trumpiau kaip 3 metus užtikrinti apsaugą nuo sugadinimo, pakeitimo ar vagystės. Taip pat jie privalo saugoti su skrydžiais susijusius įrašus, kuriuose yra: a) rizikos vertinimas ir tai patvirtinantys dokumentai, jei prieš skrydį buvo privaloma atlikti rizikos vertinimą; b) taikytos rizikos mažinimo priemonės ir c) darbuotojų, dalyvaujančių bepiločio orlaivio naudojimo, atitikties stebėjimo ir saugos valdymo veikloje, kvalifikacija ir patirtis (įrašai apie darbuotojus saugomi visą laiką, kol asmuo dirba organizacijoje, ir dar 3 metus jam palikus organizaciją)[319].

Kaip matyti iš aukščiau aptartų taisyklių, reikalavimas kaupti įrašus analizuojamose jurisdikcijose reguliuojamas skirtingai. Bendras šių taisyklių bruožas yra tas, kad reikalavimas kaupti įrašus numatytas tik vykdant pavojingesnius (specialiosios kategorijos) skrydžius, kuriems reikia atskiro nacionalinės aviacijos organizacijos leidimo. Tačiau, kokie duomenys ir kiek laiko turėtų būti kaupiami, skiriasi. Jurisdikcijų palyginimas pateiktas 7 lentelėje.

316 ICAO model UAS regulations part 101 and 102, *supra note,* 22, 102.39 straipsnis,

317 „JARUS Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, *supra note,* 273, skyrius „UAS.OPB.110 UAS Logbook“.

318 Lengvosios UAS naudotojų pažymėjimas (LUC) – tai dokumentas, patvirtinantis, jog dronų valdytojas gali pats įvertinti operacijos riziką ir vykdyti tam tikrus ar visus skrydžius civilinės aviacijos organizacijai neteikdamas atskiros deklaracijos ar be atskiro civilinės aviacijos organizacijos leidimo. Norėdamas gauti LUC, bepiločio orlaivio valdytojas nacionalinės aviacijos organizacijai privalo įrodyti, kad atitinka reikalavimus, nustatytus Reglamento (ES) 2019/947 C dalyje.

319 Reglamentas (ES) 2019/947 dalies „UAS.LUC.020. LUC turėtojo pareigos“ 5 ir 6 punktai.

7 lentelė. *Analizuojamų institucijų reikalavimas kaupti įrašus*

Analizuojamų institucijų reikalavimas kaupti įrašus		
Jurisdikcija	**Privalomai kaupiami duomenys**	**Saugojimo trukmė**
ICAO	Pilotų ir kitų įgulos narių vardai ir pavardės	12 mėn.
	Skrydžių laikas / trukmė	
	Bepiločio orlaivio techninės priežiūros veiksmai, modifikavimas ar remontas	24 mėn.
JARUS	Skrydžių trukmė	–
	Bepiločio orlaivio techninės priežiūros veiksmai	
ES	Rizikos vertinimas	36 mėn.
	Taikytos rizikos mažinimo priemonės	
	Įrašai apie darbuotojų kvalifikaciją ir patirtį	
JAV	Pareiga kaupti įrašus nenumatyta	–

Visgi siekiant išsiaiškinti, ar analizuojamų jurisdikcijų reguliavimas, numatantis privalomai kaupti duomenys, galėtų padėti apsaugoti privatumą, vertėtų apie kiekvieną informacijos kategoriją ir duomenų kaupimo trukmę padiskutuoti atskirai.

Kalbant apie ICAO reguliavimą, numatantį bepiločių orlaivių valdytojų pareigą kaupti duomenis apie pilotų ir kitų įgulos narių vardus bei pavardes, galima teigti, jog tokių duomenų kaupimas padėtų nustatyti tikruosius pažeidimo kaltininkus, jeigu bepiločio orlaivio savininkas (valdytojas) ir pilotas (ar kiti įgulos nariai) yra skirtingi asmenys, bet labiau apsaugoti nukentėjusio asmens privatumą nepadėtų. Nukentėjusiam asmeniui būtų daug svarbiau sužinoti ne pažeidėjo, o atsakingo asmens tapatybę. Jeigu reikalavimas kaupti įrašus būtų taikomas kartu su registracija, atsakomybė už bepiločiu orlaiviu padarytą žalą, panašiai kaip ir padarius eismo įvykį skolintu automobiliu, turėtų būti taikoma asmeniui, kuris nacionalinės aviacijos organizacijos registre įregistruotas jo savininku. Tuo tarpu piloto ir įgulos narių vardų bei pavardžių fiksavimas galėtų pagelbėti nebent siekiant

teisingai paskirstyti atsakomybę už padarytą žalą tarp piloto (įgulos) ir bepiločio orlaivio valdytojo. Taigi tokių įrašų privalomas kaupimas didesnės privatumo apsaugos neužtikrintų.

Tiek ICAO, tiek JARUS numato pareigą kaupti įrašus apie skrydžių laikus arba jų trukmę. Tokios informacijos kaupimas galėtų pagelbėti atkurti pažeidimų aplinkybes, tačiau tai galėtų būti tik viena iš daugelio įrodinėjimo priemonių. Vien skrydžio trukmė arba skrydžio laikas savaime apie paties skrydžio metu vykdytus veiksmus nieko nepasako, todėl apsaugant pašalinių asmenų privatumą pasitarnautų nebent derinyje su kitais skrydžio duomenimis, tokiais kaip vieta ir aukštis. Vis dėlto nei ICAO, nei JARUS, kurie yra numatę privalomą įrašų apie skrydžio laiką arba jų trukmę kaupimą, papildomai kaupti įrašų nei apie skrydžio vietą, nei apie aukštį bepiločių orlaivių valdytojams nenumatė.

Kaupti įrašus apie bepiločio orlaivio techninės priežiūros veiksmus numato tiek ICAO, tiek JARUS, tiesa, ICAO prideda duomenis apie jam atliktas modifikacijas ar remontą. Tokio pobūdžio įrašų kaupimas kur kas didesnę reikšmę turėtų skrydžių saugai negu privatumui, bet visgi galėtų netiesiogiai prisidėti prie privatumo apsaugos. Kadangi reikalavimas kaupti įrašus pagal analizuojamų jurisdikcijų reguliavimą turėtų būti taikomas tik specialiosios kategorijos skrydžiams, kurių vykdymą prižiūrėtų šalių nacionalinės aviacijos organizacijos, duomenų kaupimas apie bepiločio orlaivio techninę priežiūrą, remontą ar modifikacijas prisidėtų prie kontrolės, kad neturėtų priedų, pvz., kenkiančių duomenų ryšio saugumui, tiesiogiai perduodančių duomenis tretiesiems asmenims ar kitokiu būdu keliančių grėsmę privatumui.

ES požiūris į privalomą įrašų kaupimą gerokai skiriasi nuo ICAO ir JARUS, nes nenumato nei pareigos kaupti duomenis apie patį skrydį, nei apie bepiločio orlaivio techninę priežiūrą. Be to, ir subjektų, kurie privalo kaupti kokią nors informaciją, kur kas mažiau negu ICAO ir JARUS rekomendacijose. LUC turėtojai, kuriems taikoma pareiga kaupti duomenis, priešingai nei visi kiti specialiosios kategorijos skrydžių vykdytojai, neprivalėtų teikti nacionalinei aviacijos organizacijai kiekvieno skrydžio rizikos vertinimų, jie turėtų savarankiškai įvertinti vykdomos operacijos riziką ir kaupti duomenis apie atliktą rizikos vertinimą, rizikos mažinimo priemones, įrašus apie darbuotojų kvalifikaciją ir patirtį. Visi kiti specialiosios kategorijos skrydžių vykdytojai jokių papildomų duomenų apie skrydį kaupti neprivalo. Disertacijos autoriaus nuomone, kadangi pagal ES reglamentavimą LUC turėtojams suteikiama galimybė vykdyti visus ar tam tikrus skrydžius be atskiro civilinės aviacijos organizacijos leidimo, tai privalomas duomenų kaupimas apie atliktą rizikos vertinimą, rizikos mažinimo priemones ir darbuotojų kvalifikaciją ir patirtį jiems sukuria didesnę atskaitomybę už savo veiksmus, dėl to jie neturi daug galimybių piktnaudžiauti lengvatine LUC turėtojo padėtimi. Tokių įrašų kaupimas tiesiogiai neužkerta kelio privatumo pažeidimams, bet galėtų sumažinti jų tikimybę, jeigu poįstatyminiai teisės aktai numatytų gan griežtą LUC turėtojų kontrolę, pvz., vykdant neplaninius patikrinimus, numatant griežtas administracines poveikio priemones už LUC sąlygų nesilaikymą.

Įvertinus visų jurisdikcijų taisykles atskirai, matyti, kad įrašų kaupimas apie skrydį vykdančių asmenų, kitų įgulos narių vardus ir pavardes, taip pat apie skrydžių laikus arba jų trukmę reikšmingos įtakos privatumo apsaugai neturėtų, tačiau tam tikrą privatumo apsaugą galėtų užtikrinti įrašų kaupimas apie bepiločių orlaivių techninę priežiūrą, modifikacijas ir remontą bei duomenų, susijusių su atliktu rizikos vertinimu, saugojimas. Vis dėlto yra keletas probleminių aspektų, susijusių su tokių nuostatų taikymu praktikoje.

Pirma, iš analizuojamų taisyklių formuluočių galima suprasti, jog įrašų kaupimas priklausytų nuo pačių bepiločių orlaivių valdytojų, t. y. taisyklės numato valdytojų pareigą kaupti įrašus, bet šie patys gali pasirinkti, ką nori deklaruoti. Tokia nuostatų formuluotė sukuria galimybes kaupti įrašus pasirinktinai. Pvz., ES veikiantis bepiločio orlaivio valdytojas, kuriam išduotas LUC, žinodamas ar bent įtardamas, jog galėjo pažeisti kieno nors teisę į privatumą, gali pasirinkti ir duomenų apie tokį skrydį nekaupti, tokiu būdu nebus deklaruota, kad toks skrydis apskritai įvyko. Arba valdytojas, sąmoningai planuodamas rinkti duomenis bepiločio orlaivio priedais, kuriuos naudoti nebuvo gavęs nacionalinės aviacijos organizacijos leidimo, gali tiesiog nefiksuoti laikinos modifikacijos, o atėjus laikui atsiskaityti nacionalinei aviacijos organizacijai neteisėtą priedą tiesiog numontuoti. Privalomą įrašų kaupimą būtų galima pasiekti nebent tada, jei bepiločių orlaivių gamintojai būtų įpareigoti automatiškai kaupti tam tikrus duomenis. Pažymėtina, jog automatinio įrašų kaupimo funkcija jau ir taip integruota į populiariausių bepiločių orlaivių valdymo programėles, kurios kiekvieno skrydžio metu veda išsamų žurnalą, tačiau vartotojas žurnalo duomenis bet kada gali ištrinti. Pvz., bepiločių orlaivių gamintojo „DJI“[320] programėlė „DJI Fly“, kurią reikia įrašyti į prie pulto jungiamą išmanųjį įrenginį norint skraidinti bepilotį orlaivį, yra sukonfigūruota taip, kad automatiškai kauptų įrašus apie kiekvieną vykdomą skrydį (laiką, trukmę, aukštį, greitį ir pan.). Nors šios funkcijos išjungti programėlė neleidžia, vartotojas po skrydžio duomenis gali ištrinti.

Antra, jurisdikcijų reguliavimu siūloma privalomai kaupiamų duomenų apimtis gali būti per siaura, kad ja naudojantis būtų galima atkurti įvykdyto pažeidimo detales, tačiau praplėtus kaupiamų įrašų apimtį gali kilti papildomų privatumo grėsmių tiek pašaliniams asmenims, tiek bepiločių orlaivių valdytojams, nes padidėtų bendras atkuriamų duomenų kiekis. Taisyklės, praplečiančios reikalaujamą kaupti duomenų apimtį, galėtų būti dviejų lygmenų: 1) numatančios bepiločio orlaivio valdytojo pareigą duomenis kaupti asmeniniame archyve arba pačiame bepilotyje ir, tik gavus kompetentingos institucijos (teismo, policijos, prokuroro ir pan.) teisėtą reikalavimą, tokią informaciją suteikti; 2) numatančios bepiločio orlaivio valdytojo pareigą tuos duomenis perduoti tretiesiems asmenims (valstybei, gamintojui) periodiškai arba automatiškai. Vertėtų paanalizuoti, ar įgyvendinant

320 Gamintojo „DJI“ pavyzdys imamas neatsitiktinai. 2018 m. atliktas tyrimas parodė, jog didžiąją bepiločių orlaivių gamybos rinkos dalį užima būtent „DJI“, plačiau žr. „New Skylogic Research Market Report Uncovers Fresh Insights on Drone Industry“, UAV Coach, 2018 m. rugsėjo 19 d., https://uavcoach.com/skylogic-2018-drone-industry-benchmark/.

tiek vieną, tiek kitą įrašų kaupimo lygmenį kiltų papildomų privatumo grėsmių.

Pirmojo lygmens reguliavimas galėtų numatyti bendrą bepiločių orlaivių valdytojų pareigą kaupti didesnės apimties duomenis, panašiai kaip yra šiuo metu, tik kyla grėsmė, kad valdytojai šią informaciją kaups pasirinktinai, ją kels į nesaugias laikmenas, debesijos saugyklas. Pasirinkus tokį kelią sukaupta informacija būtų neatspari anksčiau aptartiems *agregavimo*, *identifikavimo* ir *saugumo neužtikrinimo* pažeidimams. Dar bepiločių orlaivių reguliavimas galėtų numatyti gamintojų pareigą juos gaminti su juodosiomis dėžėmis, kuriose būtų automatiškai kaupiama informacija apie jų vykdomus skrydžius. Juodoji dėžė galėtų fiksuoti tokią informaciją: skrydžio aukštį, lokaciją, greitį. Joje taip pat galėtų būti išsaugomi kelių paskutinių skrydžių vaizdo įrašai. Techninėmis priemonėmis galima būtų užtikrinti, kad juodoji dėžė nebūtų prijungta prie interneto, bet būtų prieinama tik fiziškai prie jos prisijungus laidu. Jeigu įrašai, kaupiami juodojoje dėžėje, būtų atriboti nuo interneto, jų iš asmeninių kietųjų diskų pavogti negalėtų programišiai, taip būtų išvengiama privatumo grėsmių, kurių atsiranda duomenis laikant asmeniniuose kompiuteriuose ar debesijos saugyklose. Bent jau juodojoje dėžėje esantys duomenys būtų saugūs nuo *agregavimo*, *identifikavimo* ir *saugumo neužtikrinimo* pažeidimų. Taigi privalomo įrašų kaupimo apimties padidinimas pirmuoju lygmeniu, jeigu tokie įrašai būtų kaupiami juodosiose dėžėse, ne tik nekeltų slaptų grėsmių privatumui, bet ir būtų gera privatumo apsaugos priemonė, nes įvykus pažeidimui leistų atkurti detalias to įvykio aplinkybes.

Antrojo lygmens reguliavimas papildomai galėtų numatyti bepiločių orlaivių valdytojų pareigą detalesnius įrašus periodiškai arba automatiškai perduoti valstybės institucijoms, kurios juos kauptų savo duomenų bazėse. Tokiu atveju valstybė, turėdama pakankamai duomenų ir juos interpretuodama, teoriškai galėtų užkirsti kelią pažeidimams iš anksto. Vis dėlto pažeidimai, kuriuos būtų galima tokiu būdu numatyti, turėtų būti sunkūs nusikaltimai, kurie keltų grėsmę daugelio žmonių sveikatai ar gyvybei. Tik sunku įsivaizduoti, kaip disponuodamos plačiomis informacijos duomenų bazėmis valstybės institucijos galėtų iš anksto numatyti privatumo pažeidimus. Dar daugiau, būtent periodinis ar juo labiau automatinis duomenų perdavimas būtų viena oportunistinio, visur esančio informacijos rinkimo sudedamųjų dalių, apie tai jau kalbėta aptariant agregavimo pažeidimą. Antrojo lygmens reguliavimas pernelyg varžytų tiek bepiločių orlaivių valdytojų, tiek pašalinių asmenų, kurie atsitiktinai pateko į bepiločio orlaivio vaizdo kameros objektyvą, teisę į privatumą, todėl apie jį net negalima kalbėti kaip apie privatumo apsaugos priemonę.

Taigi, didinant kaupiamų įrašų apimtį siekiama geriau apsaugoti privatumą, bet tai būtų veiksminga, jeigu duomenys būtų atriboti nuo interneto ir kaupiami pačiame bepiločiame orlaivyje, o tretiesiems asmenims tokia informacija būtų suteikiama tik gavus kompetentingos institucijos teisėtą reikalavimą.

Reikėtų aptarti, kaip jurisdikcijos siūlo reguliuoti įrašų saugojimo trukmę. Konkrečios duomenų saugojimo trukmės nustatymas turi du pagrindinius tikslus. Viena vertus, nustatyti privalomą įrašų saugojimo terminą gali būti pateisinama

tuo, kad tai užtikrintų prieigą prie svarbios informacijos, kuri gali atskleisti įvykusio pažeidimo, gedimo ar nusikaltimo detales. Kita vertus, konkreti duomenų saugojimo trukmė juose užfiksuotiems asmenims yra kaip saugiklis tiek nuo netikėtų ieškinių, tiek nuo nenuspėjamų duomenų agregacijos pasekmių ateityje. Iš analizuojamų jurisdikcijų, kurios yra numačiusios privalomą įrašų kaupimą, konkretaus duomenų kaupimo termino nenumatė tik JARUS, o ICAO nustatė 12–24 mėn., ES – 36 mėn. Disertacijos autoriaus nuomone, JARUS pozicija nenumatyti duomenų saugojimo termino nėra geras pasirinkimas privatumo atžvilgiu, nes gali sukurti tobulas sąlygas *agregavimo*, *saugumo neužtikrinimo* ir *identifikavimo* pažeidimams. ICAO ir ES pasirinkta duomenų saugojimo trukmė tikslų pasiekti padėtų, tik įstatymų leidėjams reikėtų pasirinktų vieną terminą: pasirinkus trumpesnį terminą, labiau būtų užtikrinamas antrasis tikslas, o ilgesnį – labiau pirmasis. Diskutuoti, kuris variantas yra geresnis, nėra reikalo, kadangi tiek vienas, tiek kitas užtikrintų pakankamą privatumo apsaugos lygį.

Apibendrinant galima teigti, kad reikalavimas saugoti įrašus padėtų užtikrinti tam tikrą privatumo apsaugą, bet dabar specialiuosiuose bepiločių orlaivių reguliavimo šaltiniuose kaupiamų duomenų apimtis yra per siaura, kad privalomas duomenų kaupimas būtų veiksminga privatumo apsaugos priemonė. Aukštesnį apsaugos lygį būtų galima užtikrinti numatant didinti kaupiamų duomenų apimtį. Vis dėlto turėtų būti laikomasi kelių sąlygų: 1) duomenys būtų įvedami į patį bepilotį orlaivį ir nebūtų prieinami interneto ryšiu, 2) duomenys tretiesiems asmenims būtų teikiami tik pagal teisėtą įgaliotos valdžios institucijos (teismo, ikiteisminio tyrimo pareigūno ar kt.) pareikalavimą, 3) duomenys būtų nustatytas konkretus saugojimo terminas.

2.3.5. Kvalifikacijos reikalavimai bepiločių orlaivių pilotams

Tinkama bepiločių orlaivių valdytojų kvalifikacija teoriškai galėtų suteikti tam tikrą privatumo apsaugą, jeigu privalomuose valdytojams skirtuose mokymuose būtų gan detaliai aptariamos grėsmės, kurias bepiločių orlaivių naudojimas kelia privatumui, ir duodami praktiniai patarimai, kaip jų išvengti. Vertėtų panagrinėti, ar dabartinio reguliavimo reikalavimai valdytojų kvalifikacijai yra pakankami, kad padėtų apsaugoti privatumą. ICAO reguliavimas numato, kad atvirosios kategorijos bepiločių orlaivių valdytojai prieš skrydį turėtų žinoti oro erdvės suskirstymą ir visus skrydžio vietoje galiojančius oro erdvės apribojimus arba skrydį vykdyti prižiūrint asmeniui, kuris šiuos dalykus išmano[321]. Kaip teigiama ICAO pavyzdinio reglamento komentare, tokias žinias operatoriams galėtų suteikti nacionalinės aviacijos organizacijos, skrydžių mokymų organizacijos, tinkamai kvalifikuotas pilotuojamų orlaivių pilotas ar bepiločio orlaivio pilotas[322]. Bepiločių orlaivių valdytojai, vykdantys specialiosios kategorijos skrydžius arba norintys skraidyti arčiau kaip 4 km

321 ICAO model UAS regulations part 101 and 102, *supra note,* 22, 101.15 straipsnis, 11.
322 ICAO Advisory Circular (AC) 101-1, *supra note,* 22: 8–9.

atstumu nuo oro uostų, pagal ICAO reguliavimą privalo būti licencijuoti. Tam, kad gautų licenciją, nuotolinis pilotas privalo baigti specializuotą nuotolinių pilotų mokymų kursą, skirtą tos kategorijos bepiločiams orlaiviams, kurį planuoja valdyti, arba įrodyti, kad reikiamą kvalifikaciją įgijo kitais būdais (pvz., turi piloto, skrydžio įgulos, oro kontrolės licenciją arba yra išlaikęs teorinį aviacijos žinių egzaminą ir pan.)[323].

JARUS rekomendacijose nurodo, jog atvirosios (A) kategorijos skrydžių bepiločių orlaivių operatoriai galėtų būti ugdomi trimis lygmenimis: didinant bepiločių orlaivių naudotojų informuotumą; nustatant reikalavimą įgyti pagrindines žinias apie bepiločius orlaivius ir pažeidimus, kylančius dėl piloto nepakankamo išprusimo; taikant realias sankcijas[324].

Pirmasis ugdymo lygmuo: bepiločio orlaivio naudotojas turi būti informuotas, kad naudojasi orlaiviu, kuriam taikomi tam tikri apribojimai. JARUS nuomone, vartotojų sąmoningumą galėtų didinti, jei bepiločių orlaivių pardavėjai būtų įpareigoti informuoti klientus apie naudojimo taisykles, galiojančias jų perkamam bepiločiam orlaiviui, taip pat valdžios institucijos galėtų rengti informacines kampanijas, platinti vaizdo įrašus, plakatus, pranešimus[325]. Vienoje rekomendacijoje JARUS siūlo valstybėms narėms užtikrinti, kad prie kiekvieno į rinką paleidžiamo bepiločio orlaivio būtų pridėtas informacinis lapelis arba lygiavertės elektroninės priemonės, skirtos atkreipti vartotojo dėmesį į pavojus, kylančius dėl jo valdymo, taip pat informuoti apie taikytinus teisės aktus, susijusius su aviacijos sauga, kibernetiniu saugumu, privatumu ir duomenų apsauga, atsakomybe už pažeidimus ir draudimu[326].

Antrasis ugdymo lygmuo: reikalingas sudėtingesnių, tačiau visuomenei lengvai prieinamų bepiločių orlaivių pilotams, nes šiems valdyti reikia specialių žinių. Pasak JARUS, valdytojai pagrindines žinias apie bepiločius orlaivius savanoriškai galėtų įgyti sertifikuotoje mokymo institucijoje ar naudodamiesi sertifikuota e. Mokymosi priemone ir pabaigę kursą gauti, pvz., pažymėjimą ar jam prilyginamą dokumentą, kurį pripažintų nacionalinės valdžios institucijos[327]. Viena JARUS rekomendacijų skirta aptarti, kokias žinias tokios mokymo programos turėtų suteikti bepiločių orlaivių pilotams, tarp jų minimos ir temos, susijusios su privatumo, duomenų apsaugos teisiniu reguliavimu[328].

Trečiajam ugdymo lygmeniui JARUS priskiria privalomą ugdymo reikalavimų vykdymą. Nurodo, jog realios sankcijos, proporcingos pažeidimo tipui, panašios į tas, kurios taikomos kelių eismo dalyviams, prisidėtų prie bepiločių orlaivių pilotų ugdymo[329]. Pvz., valdžios institucijos galėtų taikyti administracines sankcijas

---

323 ICAO model UAS regulations part 101 and 102, *supra note,* 22, 102.1 straipsnis, 16–17.
324 JARUS UAS Operational Categorization, *supra note,* 22: 22.
325 *Ibid.,* 22, 26.
326 JARUS Recommendation UAS RPC CAT A AND CAT B (2019): 33, jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_15_uas_rpc_cat_a_b.pdf.
327 JARUS UAS Operational Categorization, *supra note,* 22: 22.
328 JARUS Recommendation UAS RPC CAT A AND CAT B, *supra note,* 325: 22.
329 JARUS UAS Operational Categorization, *supra note,* 22: 22.

už tai, kad pilotas naudojasi atitinkamos kategorijos bepiločiu orlaiviu, nors nėra išklausęs privalomųjų kursų, arba bepiločių orlaivių prekiautojui už tai, kad šis vartotojui nepateikė išsamios informacijos, kaip juo naudotis nepažeidžiant kitų asmenų teisių.

Dar vienas papildomas ugdymo lygmuo, pasak JARUS, galėtų būti skirtas labai sudėtingų, didelių bepiločių orlaivių, pritaikytų komerciniam keleivių transportavimui, valdytojams. Jie būtų privalomai licencijuojami, panašiai kaip ir įprastų orlaivių pilotai[330]. Licencijai gauti bepiločio orlaivio pilotas turėtų išklausyti privalomą atitinkamos kategorijos kursą ir išlaikyti teorinį bei praktinį egzaminus[331].

Pagal ES reguliavimą reikalavimas įgauti papildomą kvalifikaciją valdytojams netaikomas, jeigu jie naudoja labai lengvus bepiločius orlaivius. Valdytojai, kurių bepilotis orlaivis sveria mažiau kaip 250 g (C0 klasė arba privačiai pagaminti), turi būti susipažinę tik su gamintojo naudojimo vadovu. Vis dėlto visi kiti atvirosios kategorijos skrydžius (A1, A2 ir A3 pakategorės) vykdantys pilotai privalo būti susipažinę su gamintojo vadovu, baigti nuotolinius mokymus, kuriuos organizuoja nacionalinė civilinės aviacijos organizacija, ir sėkmingai išlaikyti nuotolinį teorinių žinių egzaminą. Gamintojo vadove privalo būti atitinkamas visų pavojų, kylančių naudojant bepilotį orlaivį, aprašymas[332]. Nuotoliniam pilotui, baigusiam tokius kursus, turėtų būti žinomi šie dalykai: skrydžių sauga, oro erdvės apribojimai, aviacijos reguliavimas, žmogaus galimybių ribos, veiklos procedūros, bendrosios žinios apie bepiločius orlaivius, privatumo ir duomenų apsauga, draudimas, saugumas[333].

Nuotoliniai pilotai, norintys vykdyti A2 pakategorės skrydžius, turi papildomai patys pasimokyti skraidinti bepiločius orlaivius nuošalesnėse vietose (150 m atstumu nuo tankiai apgyvendintų vietų) ir išlaikyti papildomą kompetentingos institucijos (pvz., nacionalinės aviacijos organizacijos) rengiamą teorinių žinių egzaminą. Per egzaminą patikrinamos operatoriaus žinios apie meteorologiją, bepiločio skrydžio vykdymą, techninius ir su naudojimu susijusius ant žemės gresiančios rizikos mažinimo būdus[334].

Kai vykdomas specialiosios kategorijos skrydis, pagal ES reglamentavimą valdytojui reikalinga kvalifikacija priklauso nuo vykdomos operacijos. Jeigu vykdomas skrydis nepatenka į standartinį scenarijų, valdytojai, atlikę rizikos įvertinimą, patys turės įvertinti, kokių kvalifikacijos reikalavimų gali reikėti planuojamam vykdyti skrydžiui, ir savo siūlymą turės pateikti nacionalinei aviacijos organizacijai, kuri įvertins turimos kvalifikacijos tinkamumą. Tačiau visais atvejais pilotai turi turėti bent tokius gebėjimus: a) taikyti veiklos procedūras (įprastas, nenumatytų aplinkybių ir avarines procedūras, skrydžio planavimo, patikrinimo

330 *Ibid.,* 31, 42.
331 JARUS FCL Recommendation, (2015): 20–21.
332 Reglamentas (ES) 2019/945, priedas.
333 Reglamentas (ES) 2019/947, A priedo dalis.
334 Reglamentas (ES) 2019/947, A priedo skyrius „aus.OPEN.030. UAS naudojimas A2 pakategorės skrydžiams vykdyti“.

prieš skrydį ir po skrydžio); b) valdyti oro navigacijos ryšį; c) valdyti bepiločio orlaivio skrydžio trajektoriją ir automatizavimą; d) vadovavimo, bendradarbiavimo ir savitvardos; e) problemų sprendimo ir sprendimų priėmimo; f) situacijos suvokimo; g) darbo krūvio valdymo; h) koordinavimo arba perdavimo, kaip tinkama[335]. Jeigu operacija patenka į standartinį scenarijų, nuotolinis pilotas, taip pat kaip ir per A2 pakategorės operaciją, turės baigti ir sėkmingai išlaikyti nuotolinius mokymo kursus, išlaikyti kompetentingos institucijos rengiamą teorinių žinių egzaminą. Skirtumas tik toks, kad norėdami vykdyti specialiosios kategorijos skrydžius pilotai papildomai turės baigti ir atitinkamo standartinio scenarijaus praktinių įgūdžių mokymus[336].

JAV komercinius ir rekreacinius skrydžius reglamentuoja skirtingi teisės aktai, bet nepriklausomai nuo to, ar skrydis vykdomas komerciniais, ar rekreaciniais tikslais, bepiločio orlaivio pilotas privalo išlaikyti aeronautikos žinių testą. Šiuo metu aeronautikos žinių testas laikinai privalomas tik komerciniais tikslais skrydžius vykdantiems subjektams[337], tačiau vėliau bus privalomas ir bepiločių orlaivių pilotams, skraidinantiems rekreaciniais tikslais[338]. Žinių patikrinimas komerciniais tikslais skrydžius vykdantiems subjektams apima šias aeronautikos žinių sritis: 1) taisyklės, susijusios su nedidelių bepiločių orlaivių kvalifikacijos suteikimo teisėmis, apribojimais ir skrydžio vykdymu, 2) oro erdvės klasifikavimo ir eksploatavimo reikalavimai bei skrydžio apribojimai, turintys įtakos nedidelių bepiločių orlaivių skrydžiams; 3) aviacijos orų šaltiniai ir orų poveikis nedidelių bepiločių orlaivių skrydžiams, 4) nedidelių bepiločių orlaivių apkrova ir našumas, 5) avarinės procedūros, 6) įgulos išteklių valdymas, 7) radijo ryšio procedūros, 8) nedidelių bepiločių orlaivių našumo įvertinimas, 9) narkotikų ir alkoholio fiziologinis poveikis, 10) aeronautinių sprendimų priėmimas ir vertinimas, 11) operacijos oro uostuose, 12) priežiūros ir patikrinimo procedūros prieš skrydį[339].

---

335 Reglamentas (ES) 2019/947, 8 straipsnio 2 dalis.

336 Standartiniai scenarijai šiuo metu, kai rašoma disertacija, dar tik kuriami ir apie juos galima sužinoti tik nagrinėjant EASA publikuojamus paruošiamuosius dokumentus. Apie planuojamus Reglamento (ES) 2019/945 ir Reglamento (ES) 2019/947 pakeitimus, susijusius su standartiniais scenarijais, EASA yra publikavusi Nuomonę, žr. European Union Aviation Safety Agency, „Opinion No 05/2019 – Standard scenarios for UAS operations in the 'specific' category", (2019): 8–9, 17.

337 CFR 14 skyriaus 107.61 straipsnis; Federal Aviation Administration, „Remote Pilot – Small Unmanned Aircraft Systems (Certification and Recurrent Knowledge Testing) Airman Certification Standards", Flight Standards Service Washington, DC 20591, 2018; www.faa.gov/training_testing/testing/acs/media/uas_acs.pdf, „Policy Document Library", template, žiūrėta 2020 m. spalio 14 d., https://www.faa.gov/uas/resources/policy_library/#107.

338 Reauthorization Act of (2018): 22554, 8 punktas, „Aeronautical Knowledge and Safety Test Updates", template, žiūrėta 2020 m. spalio 14 d., https://www.faa.gov/uas/recreational_fliers/knowledge_test_updates/.

339 Federal Aviation Administration, „Advisory Circular No. 107-2" (AC 107-2), (2016): 6–4, www.faa.gov/documentlibrary/media/advisory_circular/ac_107-2.pdf.

Kaip matyti iš atliktos analizės, visos jurisdikcijos numato tam tikrus kvalifikacijos reikalavimus bepiločių orlaivių valdytojams, pilotams ar įgulos nariams. Tačiau reikalavimą į bepiločių orlaivių valdytojų mokymų programas integruoti temas apie privatumą ir duomenų apsaugą arba bent jau informaciniuose lapeliuose įsigyjant bepilotį orlaivį išvardyti pavojus, kylančius privatumui ir duomenų apsaugai, numato tik JARUS ir ES, o pagal ICAO ir JAV reguliavimą bepiločių orlaivių valdytojams pakanka žinoti su skrydžio sauga susijusius dalykus. Taigi toliau analizę galima susiaurinti ir aptarti JARUS bei ES numatytas priemones.

Pažymėtina, jog pilotų kvalifikacijos taisyklių atžvilgiu JARUS ir ES reguliavimas yra labai panašus. JARUS rekomendacijose numatyti trys ugdymo lygmenys, iš kurių pirmasis ir antrasis praktiškai yra įgyvendinti ES. Pirmąjį lygmenį ES įgyvendina reikalavimas, nurodantis prie bepiločio orlaivio pridėti gamintojo vadovą, kuriame, *inter alia,* būtų ir visų pavojų, kylančių naudojant bepilotį orlaivį, aprašymas. Antrąjį lygmenį įgyvendina reikalavimas daugumai bepiločių orlaivių valdytojų baigti internetinius mokymus, išlaikyti internetinį egzaminą ir papildomai kompetentingos institucijos rengiamą teorinių žinių egzaminą. Trečiojo ugdymo lygmens specialusis ES bepiločių orlaivių reglamentavimas neaptaria, jo įgyvendinimas paliktas valstybėms narėms. Kiekvieną iš ugdymo lygmenų vertėtų aptarti atskirai ir paanalizuoti, kiek kiekvienas iš jų galėtų prisidėti prie privatumo apsaugos.

Pirmojo lygmens ugdymas, pasak JARUS, galėtų būti iš esmės dviejų rūšių: 1) prie įsigyjamo bepiločio orlaivio pridedant gamintojo vadovą, 2) rengiant bendras informacines kampanijas. Kalbant apie gamintojo vadovą kaip privatumo apsaugos priemonę, manytina, kad jis galėtų būti veiksmingas tik tuo atveju, jeigu jame pateikta informacija būtų įsimintina, tikslinga ir praktiška. Atlikus psichologinius tyrimus nustatyta, kad vartotojams kartu su produktu pateikiamų bukletų suprantamumas ir informacijos įsiminimas labai priklauso nuo pateikimo būdo, jiems svarbus ne tik turinys, bet ir šriftas, paveikslėliai[340]. Todėl gamintojo vadovai turi atitikti tam tikrus pateikimo formos kriterijus, kurie vartotojui padėtų geriau įsiminti dokumente esančią informaciją. Žinoma, svarbi ne tik pateikimo forma, bet ir turinys. Tačiau privatumo keliamas grėsmes ir jų prevencijos priemones vartotojui gali būti žymiai sunkiau suvokti negu techninius dalykus, tokius kaip naudojimo, techninės priežiūros nurodymai, nesklandumų šalinimo procedūros ar naudojimo apribojimai. Tai gali lemti įvairios priežastys, pvz., neišsami informacija, ribotas racionalumas ir sistemingi psichologiniai nukrypimai nuo racionalumo[341]. Vis dėlto bepiločio valdytojui nebūtina suprasti visų pasekmių, kurias

340 Carl Martin Allwood ir Tomas Kalén, „Evaluating and improving the usability of a user manual", *Behaviour & Information Technology* 16, 1 (1997): 43–57, Stephen L. Young ir Michael S. Wogalter, „Comprehension and memory of instruction manual warnings: Conspicuous print and pictorial icons", *Human Factors* 32, 6 (1990): 637–649.

341 Alessandro Acquisti ir Jens Grossklags, „Privacy and rationality", *Privacy and Technologies of Identity* (Springer, 2006), 15–29.

gali sukelti skrydžių vykdymas tam tikrais būdais, jam užtenka tik žinoti, kaip turėtų nesielgti arba kaip turėtų elgtis skrydžio metu, kad užtikrintų geresnę pašalinių asmenų privatumo apsaugą. Kitaip tariant, gamintojo vadove bepiločio orlaivio valdytojui galima būtų pateikti gerosios ir blogosios praktikos naudojimosi bepiločiu pavyzdžius, kurie tikslingai padėtų valdytojui pasirinkti elgesio būdą, o ne bendrą informaciją, kad valdytojas privalo nepažeisti pašalinių asmenų privatumo, nes bepiločio operatoriui iš abstraktaus reikalavimo gali būti sunku suvokti, kokias pasekmes privatumui gali sukelti jo veiksmai.

Informacinių kampanijų organizavimas, kaip privatumo apsaugos priemonė, galėtų pasiteisinti, bet tik tuo atveju, jeigu būtų atliekamas kompetentingai. Iš mokslinių tyrimų matyti, kad vien suteikus daugiau informacijos nebūtinai keičiasi žmonių įsitikinimai ar elgesys[342]. Pasak A. Christiano ir A. Neimand, gerą informacinę kampaniją sudaro keturi elementai: kuo siauresnė auditorija, patraukl ūs pranešimai, raginantys veikti, pokyčių teorijos turėjimas ir tinkami pranešėjai. Vykdant informacines kampanijas netinkamai, galimi priešingi rezultatai: pasiekti visai kitą auditoriją, sukelti neigiamas visuomenės reakcijas arba netgi kam nors pakenkti[343]. Taigi, informacinė kampanija, kurios tikslas – sumažinti privatumo pažeidimų, kurie įvykdomi bepiločiais orlaiviais, tikimybę, turėtų remtis socialinės psichologijos tyrimais ir būti iš anksto gerai apgalvota.

Taigi pirmasis ugdymo lygmuo galėtų būti gera prevencinė priemonė, tačiau gamintojo vadovų ir informacinių kampanijų pateikimo forma bei turinys turėtų būti paremti patyrusių bepiločių orlaivių pilotų rekomendacijomis ir atitinkamais moksliniais tyrimais.

Antrojo lygmens ugdymas, t. y. privalomi internetiniai mokymai ir teorijos egzaminai, – gali būti veiksminga privatumo pažeidimų prevencijos priemonė, bet tik tuo atveju, jeigu mokymo programose informacija apie privatumo ir asmens duomenų apsaugą būtų pateikiama kokybiškai. Per privalomus mokymus būtų galima pasiekti kur kas aukštesnį bepiločių orlaivių valdytojų sąmoningumo lygį, nes jų metu informacijos pateikiama žymiai daugiau. Kadangi per mokymai gvildenamos įvairios temos, svarbu informaciją apie privatumą pateikti taip, kad ji būtų įsimintina, tikslinga ir praktiškai naudinga.

Sankcijų taikymas, kai nesilaikoma išsilavinimo reikalavimų (trečiasis ugdymo lygmuo), manytina, taip pat mažintų bepiločių orlaivių valdytojų, kurie skrydžius vykdo be reikiamo išsilavinimo, skaičių. Dėl to sumažėtų atvejų, kai pilotai skrydį vykdo nežinodami metodų, kaip išvengti privatumo pažeidimų. Politikos

342 Julia Daisy Fraustino ir Liang Ma, „CDC's Use of Social Media and Humor in a Risk Campaign – „Preparedness 101: Zombie Apocalypse", *Journal of Applied Communication Research* 43, 2 (2015): 222–241, https://doi.org/10.1080/00909882.2015.1019544; Jennifer L. Jacquet ir Daniel Pauly, „The rise of seafood awareness campaigns in an era of collapsing fisheries", *Marine Policy* 31, 3 (2007): 308–13; Dan M. Kahan, „A risky science communication environment for vaccines", Science 342, 6154 (2013): 53–54.

343 Ann Christiano ir Annie Neimand, „Stop raising awareness already", *Stanford Social Innovation Review* 15, 2 (2017): 34–41.

formuotojai reguliariai taiko finansines bausmes ir kitas poveikio priemones, kad atgrasytų žmones nuo nepageidaujamų veiksmų (tokių kaip greičio viršijimas, šiukšlinimas ar mokesčių vengimas), darydami prielaidą, jog nepageidaujamą elgesį susiejus su bausme toks elgesys taps mažiau patrauklus[344]. Daugybė atliktų mokslinių tyrimų atskleidžia, kad tokios politikos formuotojų prielaidos turi pagrindą, t. y. bausmė išties gali gerokai sumažinti nepageidaujamo elgesio dažnumą[345]. Išsilavinimo reikalavimų nesilaikymas kaip pažeidimas nėra labai pavojingumas, todėl už šio reikalavimo nesilaikymą galėtų būti taikomos švelnios administracinės nuobaudos, pvz., įspėjimas, viešieji darbai ar bauda.

Kaip matyti iš šiame skyriuje atliktos analizės, tik dvi iš analizuojamų jurisdikcijų (JARUS ir ES) yra numačiusios reikalavimą bepiločių orlaivių valdytojus privalomai šviesti apie grėsmes, kylančias privatumui ir duomenų apsaugai. JARUS ir ES požiūriai šiuo klausimu sutampa, o ES jau yra numačiusi du iš trijų ugdymo lygmenų, aptartų JARUS rekomendacijose. Apibendrinant diskusiją apie siūlomus bepiločių orlaivių valdytojų kvalifikacijos kėlimo variantus pažymėtina, kad reikalavimai prie įsigyjamo bepiločio orlaivio pridėti naudotojo vadovą, rengti informacines kampanijas, didesnių pajėgumų bepiločių orlaivių valdytojus įpareigoti baigti specialius mokymus bei sankcijų taikymas už išsilavinimo reikalavimų nesilaikymą, gali būti veiksmingos privatumo apsaugos priemonės, bet jų įgyvendinimas neturėtų būti formalus. Gamintojo vadovuose ir privalomuose mokymuose informacija turėtų būti įsimintina, tikslinga ir praktiškai pritaikoma privatumo apsaugai. Informacines kampanijas reikėtų skirti kuo siauresnei auditorijai, skelbiant patrauklius pranešimus, raginančius veikti, ir įvardijant, ką konkrečiai reikėtų keisti, taip pat labai svarbu, kad idėjas pristatytų gerai parengti pranešėjai.

---

344 Gary S. Becker, „Crime and punishment: An economic approach“, *The economic dimensions of crime* (Springer, 1968), 13–68; Robert Cooter, „Expressive law and economics“, *The Journal of Legal Studies* 27, S2 (1998): 585–607.

345 Roland Bénabou ir Jean Tirole, „Incentives and prosocial behavior“, *American economic review* 96, 5 (2006): 1652–1678; Daniel Eek ir kt., „Spill-over effects of intermittent costs for defection in social dilemmas“, *European Journal of Social Psychology* 32, 6 (2002): 801–13; Ernst Fehr ir Armin Falk „Psychological Foundations of Incentives“, *European Economic Review* 46, 4–5 (2002): 687–724; Christopher McCusker ir Peter J. Carnevale, „Framing in resource dilemmas: Loss aversion and the moderating effects of sanctions“, *Organizational Behavior and Human Decision Processes* 61, 2 (1995): 190–201; Elinor Ostrom, James Walker ir Roy Gardner, „Covenants with and without a sword: Self-governance is possible“, *American political science Review* 86, 2 (1992): 404–417; Mark Van Vugt ir David De Cremer, „Leadership in social dilemmas: The effects of group identification on collective actions to provide public goods.“, *Journal of personality and social psychology* 76, 4 (1999): 587; Arjaan Wit ir Henk A. Wilke, „The presentation of rewards and punishments in a simulated social dilemma.“, *Social Behaviour,* (1990); Toshio Yamagishi, „The provision of a sanctioning system as a public good.“, *Journal of Personality and social Psychology* 51, 1 (1986): 110.

2.3.6. Reikalavimas atlikti rizikos vertinimą

Rizikos vertinimo procedūra prieš vykdant skrydį taip pat teoriškai galėtų apsaugoti privatumą, jeigu pagal ją būtų privaloma įvertinti ir galimas grėsmes privatumui. Visų analizuojamų jurisdikcijų reguliavimas turi nuostatas, kurios įtvirtina reikalavimą, prieš vykdant specialiosios kategorijos skrydžius, atlikti rizikos vertinimą ir kurios paremtos iš esmės ta pačia Specialiųjų operacijų rizikos vertinimo (SORA) koncepcija, kurią išplėtojo JARUS[346]. SORA iš esmės susideda iš trijų pagrindinių etapų: 1) antžeminės rizikos klasės (GRC) nustatymo, 2) oro rizikos klasės (ARC) nustatymo, 3) antžeminės ir oro rizikos įvertinimų konsolidavimo, išvadų nacionalinei aviacijos organizacijai pateikimo. Rekomendacijose detalizuojama, jog nustatant GRC yra svarbu įvertinti, kokia tikimybė, kad ant žemės esančio žmogaus užkris bepilotis orlaivis, o nustatant ARC yra svarbu įvertinti, kokia tikimybė, kad bepilotis orlaivis skrydžio metu susidurs su kitais orlaiviais. Žala, kurios SORA turėtų padėti išvengti, yra mirtini sužeidimai ir kritiniai infrastruktūros pažeidimai[347], o galimų rizikų privatumui SORA įvertinti nereikalauja[348]. ICAO reguliavimas grindžiamas rizikos vertinimo taisyklėmis, kurios nustatytos Pavyzdinio bepiločių orlaivių reglamento 102.23[349] straipsnyje, ES – Įgyvendinimo reglamento 11 straipsnyje[350], o JAV – CFR 14 antraštės 107.49 straipsnyje[351]. Tačiau ir šiose jurisdikcijose SORA procedūros apsiriboja rizikos skrydžio saugai įvertinimu, o papildomai vertinti rizikos, kylančios privatumui, nereikalauja.

Taigi, tokia rizikos vertinimo procedūra, kokią numato dabartinis specialusis analizuojamų jurisdikcijų bepiločių orlaivių reguliavimas, vargu ar galėtų suteikti tinkamą privatumo apsaugą, nes pagal jį bepiločių orlaivių operatoriai neprivalo įvertinti rizikos privatumui, kurią gali kelti vykdomas skrydis. Vis dėlto rizikos vertinimas, kaip priemonė, galėtų būti veiksminga privatumui apsaugoti, jeigu prieš vykdydami tam tikrus skrydžius operatoriai būtų įpareigoti įvertinti ir galimą žalą privatumui. Panašią priemonę iš esmės numato ES duomenų apsaugos teisės aktai[352].

2.3.7. Nuotolinio identifikavimo priedai

Specialusis bepiločių orlaivių reguliavimas numato dar vieną priemonę, teoriškai galinčią užtikrinti tam tikrą privatumo apsaugą, – tai reikalavimas, kad prie bepiločių orlaivių būtų pritaisyti nuotolinio identifikavimo priedai, kurie padėtų nukentėjusiems tretiesiems asmenims nustatyti pažeidėją, nors fiziškai jo ir

346 „JARUS guidelines on Specific Operations Risk Assessment (SORA)“, No. JAR-DEL-WG6-D.04, 2019-01-30.
347 *Ibid.,* 17.
348 *Ibid.,* 12, 1.3 poskyrio e dalis.
349 ICAO model UAS regulations part 101 and 102, *supra note,* 22: 102.23 straipsnis.
350 Reglamento (ES) 2019/947 11 straipsnis.
351 CFR section 14, part 107 paragraph 107.49.
352 Žr. disertacijos 4.3.4 poskyrį.

nematytų. Vis dėlto vertėtų aptarti, kaip analizuojamų jurisdikcijų specialusis bepiločių orlaivių reguliavimas kelia reikalavimą įdiegti tokias technologijas. Tiktai ICAO į savo reguliavimą nėra įtraukusi nuotolinio identifikavimo priedų, o kitos analizuojamos jurisdikcijos vienaip ar kitaip apie juos užsimena.

JARUS rekomenduoja šalims numatyti privalomą elektroninį identifikavimą (galimybę identifikuoti skrendantį bepilotį orlaivį be tiesioginės fizinės prieigos prie jo[353]) bepiločių, kurių svoris didesnis kaip 250 g[354]. Kokią informaciją turėtų transliuoti elektroninio identifikavimo priedas, JARUS savo rekomendacijose nedetalizuoja.

Reglamento (ES) 2019/945 priedo 6 dalis numato, kad tiesioginio nuotolinio identifikavimo priedas realiuoju laiku visą skrydžio laiką turi užtikrinti, kad iš bepiločio orlaivio pagal atvirą dokumentais patvirtintą duomenų perdavimo protokolą periodiškai būtų tiesiogiai perduodami identifikavimo duomenys, kuriuos tame ryšio diapazone galėtų tiesiogiai priimti esantys mobilieji įrenginiai. Duomenys, kuriuos turėtų be perstojo transliuoti skrydį vykdantis bepilotis orlaivis yra: 1) bepiločio orlaivio naudotojo registracijos numeris, unikalus fizinis priedo serijos numeris, 2) bepiločio orlaivio geografinė padėtis ir jo aukštis virš paviršiaus arba pakilimo vietos, 3) bepiločio orlaivio kursas, išmatuotas laikrodžio rodyklės judėjimo kryptimi nuo tikrosios šiaurės krypties, ir greitis žemės atžvilgiu, 4) nuotolinio piloto geografinė padėtis arba, jeigu ji nežinoma, pakilimo vietos geografinė padėtis. Tiesa, šis reikalavimas netaikomas bepiločiams orlaiviams, kurių svoris mažesnis kaip 250 g (C0 klasė), aviamodeliams (C4 klasė) ir privačiai sukonstruotiems bepiločiams orlaiviams.

JAV formalus reguliavimas reikalavimą turėti nuotolinius identifikavimo priedus numato visiems bepiločiams orlaiviams. Išimtys taikomos tik tada, jeigu skrydis vykdomas specialiose FAA geografiškai apibrėžtose identifikavimo zonose. Jeigu skrydis nevykdomas vadovaujantis išimtimi, pagal JAV reguliavimą bepiločių orlaivių valdytojai turi du pasirinkimus, kad atitiktų nuotolinio identifikavimo reikalavimą: (1) bepilotis orlaivis privalo turėti standartinį nuotolinį identifikavimo priedą, (2) bepilotis orlaivis privalo turėti nuotolinio identifikavimo modulį[355].

Pirmasis ir antrasis atvejai labai panašūs. Vienintelis skirtumas tai, kad pirmuoju atveju nuotolinio identifikavimo priedas turėtų būti neatskiriama bepiločio orlaivio dalis, t. y. bepilotis orlaivis turėtų būti pagamintas su integruotu nuotolinio identifikavimo priedu. Antruoju – transliacijos modulis gali būti atskiras įrenginys, prijungtas prie bepiločio orlaivio, t. y. nuotolinio identifikavimo priedas neintegruotas į bepilotį orlaivį, jį gaminant. Bepilotis pagal abi sąlygas skrydžio metu turėtų transliuoti nustatyto turinio duomenis radijo ryšiu (arba

353 „Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, *supra note,* 268, skyriaus „Recommended JARUS-OPS A & B“ 2 straipsnio h punktas.

354 *Ibid.,* 5 straipsnis.

355 „Remote Identification of Unmanned Aircraft“, Final rule, Federal Aviation Administration (FAA), FAA-2019-1100, 86 FR 4390, 2021 m. sausio 15 d.

naudojant belaidį ryšį ar „Bluetooth“ technologiją) ir transliacija turėtų būti suderinama su šiuolaikiniais asmeninio naudojimo bevieliais įrenginiais. Duomenys, kuriuos turėtų be perstojo transliuoti skrydį vykdantis bepilotis orlaivis yra: 1) bepiločio orlaivio registracijos numeris (identifikavimo modulio atveju – modulio serijinis numeris), 2) bepiločio orlaivio geografinė padėtis ir greitis, 3) valdymo pulto geografinė padėtis (identifikavimo modulio atveju – pakilimo vietos geografinė padėtis), 4) laiko žyma, 5) avarinės būklės indikatorius (identifikavimo modulio atveju šis reikalavimas netaikomas). Skrydis pagal pirmąją sąlygą galėtų būti vykdomas tiek VLOS, tiek BVLOS. Pagal antrąją – tik VLOS.

Iš atliktos reguliavimo šaltinių analizės matyti, jog detaliausiai nuotolinio identifikavimo priedai reglamentuoti ES ir JAV. JARUS ir ES taisyklės vadovaujasi ta pačia logika, skirtumas tik toks, kad ES reguliavimas detalesnis, todėl toliau aptariant JARUS ir ES reguliavimą pakaks ES pavyzdžio.

Nagrinėjant ES ir JAV reguliavimą matyti, kad esminės jų nuotolinio identifikavimo priedų reguliavimo nuostatos labai panašios. Nuotolinio identifikavimo priedas tiek ES, tiek JAV nustatyto turinio duomenis privalo transliuoti bepiločio orlaivio skrydžio zonoje, juos tame ryšio diapazone tiesiogiai priimtų esantys mobilieji įrenginiai. Privalomų transliuoti duomenų turinys ES ir JAV praktiškai identiškas. Tiesa, esama tam tikrų skirtumų. ES nuotolinio identifikavimo priedų privalomumą sieja praktiškai išimtinai su bepiločio orlaivio svoriu, t. y. jeigu bepilotis sveria mažiau kaip 250 g, jam nuotolinio identifikavimo priedai neprivalomi. JAV taisyklėse nuotolinio identifikavimo priedų privalomumas siejamas su registracijos reikalavimu. Kadangi registruoti JAV privaloma net ir bepiločius orlaivius, kurie naudojami rekreaciniams tikslams, nuotoliniai identifikavimo priedai taip pat privalomi visiems bepiločiams. Skirtingai nei ES, JAV skrydžius be nuotolinio identifikavimo priedo galima vykdyti specialiai FAA geografiškai apibrėžtose vietovėse (populiariai vadinamose „smėlio dėžėmis“)[356].

Vertinant ES ir JAV reguliavimą privatumo kontekste, disertacijos autoriaus nuomone, tiek ES, tiek JAV taisyklės turi tam tikrų trūkumų.

Pagal ES reglamentus bepiločiai orlaiviai iki 250 g svorio neprivalo turėti nuotolinio identifikavimo priedų, bet privalo būti registruojami, jeigu jie gali fiksuoti asmens duomenis. Tai reiškia, kad potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai, nors ir būtų registruoti, bet nuotoliniu būdu būtų neatpažįstami nukentėjusiems tretiesiems asmenims. Disertacijos autoriaus vertinimu, ES taisyklėse šiuo požiūriu yra spraga, kurią būtų galima ištaisyti nuotolinių identifikavimo priedų privalomumą siejant ne tik su bepiločio orlaivio svoriu, bet ir (kaip ir registracijos nuostatų atveju) su bepiločio orlaivio galimybe fiksuoti asmens duomenis. Tą patį rezultatą būtų galima pasiekti ir tiesiog įtvirtinant, jog nuotolinio identifikavimo priedai privalomi visiems bepiločiams, kuriems taikomas

356 Sally French, „These 8 States Are the Perfect Sandbox for Drones“, *The Drone Girl* (blog), 2022 m. rugsėjo 29 d., https://www.thedronegirl.com/2022/09/29/drone-sandbox-mercatus/.

registracijos reikalavimas. Būtent tokios nuostatos laikosi dabartinis JAV specialusis bepiločių orlaivių reguliavimas. Įvedus tokią taisyklę, galėtų išaugti nedidelių bepiločių orlaivių kainos, nes juos turėtų gaminti su nuotolinio identifikavimo priedais, tačiau tai galėtų sustabdyti technologines gamintojų lenktynes. Apie tai jau buvo kalbėta anksčiau analizuojant nuostatas, numatančias reikalavimą registruoti bepiločius orlaivius (jų valdytojus)[357].

JAV reguliavimo atveju problemų gali kilti įgyvendinant „smėlio dėžių" išimtį. JAV modelis, skirtas tik nedideliems bepiločiams orlaiviams be nuotolinio identifikavimo priedų, atrodo visai perspektyvus. Vis dėlto realybėje, jeigu bepiločio orlaivio, neturinčio nuotolinio identifikavimo priedo, valdytojas nuspręstų nesilaikyti nustatytų „smėlio dėžės" ribų, tiek nukentėjusiems asmenims, tiek teisėsaugos pareigūnams gali būti sunku nustatyti pažeidėjo tapatybę. Taigi JAV FAA siūlomo modelio rezultatas gali būti panašus, kaip ir ES reguliavimo – potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai būtų sunkiai atpažįstami nuotoliniu būdu, todėl jų valdytojai už privatumo pažeidimus gali būti nebaudžiami. Visgi JAV atvejis kiek skiriasi, nes ES skrydžių vykdymas neregistruotais ir nuotolinio identifikavimo priedų neturinčiais bepiločiais orlaiviais yra įteisintas, o JAV skrydžių vykdymas už „smėlio dėžės" ribų būtų nelegalus. Todėl asmenų, kurie ryžtųsi sąmoningai pažeisti teisės aktus, būtų ženkliai mažiau, nei tada, kai skrydžiai tokiais bepiločiais orlaiviais būtų legalizuoti. Lemiamą reikšmę įgyvendinant JAV reguliavimą turėtų nuobaudų už pažeidimus griežtumas, juk retas entuziastas drįstų skraidinti savo bepilotį orlaivį neleistinose vietose rizikuodamas gauti didelę baudą. Praktika iki šiol rodo, jog baudos už bepiločių orlaivių taisyklių nesilaikymą skiriamos gana didelės[358]. Kita išeitis, kurios dar nėra JAV taisyklėse, galėtų būti technologinė – t. y. gamintojai galėtų būti įpareigoti bepiločius orlaivius iš anksto užprogramuoti taip, kad negavus kompetentingo subjekto leidimo jais nepavyktų netgi pakilti zonose, kur tokiems bepiločiams orlaiviams vykdyti skrydžius draudžiama.

Privatumo apsaugos požiūriu tiek ES, tiek JAV reguliavimas kritikuotinas ir dėl duomenų perdavimo (transliavimo) formos. Pagal ES ir JAV bepiločių orlaivių reguliavimą nustatyto turinio duomenis nuotolinio identifikavimo priedas skrydžio metu privalo transliuoti tik toje vietoje, kur vykdomas skrydis. Nekvestionuotina, jog toks pagrindinių duomenų transliavimas tam tikru mastu būtų palankus privatumo apsaugai. Pažeidėjas išties teoriškai galėtų būti nuotoliniu būdu identifikuojamas, tačiau pažeidėjo atpažinimas būtų realus tiktai tuomet, jeigu: (1) pažeidimo auka savo išmaniajame įrenginyje yra atsisiuntusi specialią bepiločių orlaivių

357 Žr. disertacijos 2.3.3 poskyrį.

358 Jonathan Rupprecht, „FAA Has Busted Multiple Drone Flyers. Here Are The Expensive Results.", *Forbes,* žiūrėta 2022 m. gruodžio 19 d., https://www.forbes.com/sites/jonathanrupprecht/2022/01/18/faa-busted-multiple-drone-flyers-here-are-the-expensive-results/. (Straipsnyje rašoma, jog už bepiločių orlaivių komercinius skrydžius, atliktus per tam tikrą laikotarpį, jų valdytojui skirta net 1,9 mln. JAV dolerių bauda. Nustatyta ir daugiau atvejų, kai FAA skyrė baudas, kurios siekė 16 000–182 000 JAV dolerių.)

identifikavimo programėlę[359], (2) bepiločio orlaivio skrydžio metu pastebėjo galimą pažeidimą, (3) kol bepilotis orlaivis dar yra ryšio zonoje, spėjo nurašyti ar padaryti jo momentinę identifikavimo duomenų nuotrauką. Taigi pažeidimo aukai reikėtų imtis aktyvių veiksmų, kad pažeidėją užfiksuotų įvykio vietoje. Vis dėlto dažniausiai tokių pažeidėjų identifikavimas būtų tik atsitiktinis. Kaip jau minėta, išskirtinė bepiločių orlaivių savybė yra jų nepastebimumas, dėl to individai gali net nepastebėti, jog šalia jų yra stebėseną vykdantis bepilotis orlaivis[360]. Slaptos stebėsenos atvejais vietinis pagrindinių bepiločio orlaivio (jo valdytojo) identifikavimo duomenų transliavimas nuotoliniu būdu, disertacijos autoriaus nuomone, nebūtų veiksmingas.

Viena išeičių galėtų būti identifikavimo duomenų transliavimas ne tik vietiniu būdu, bet ir internetu centrinei valdžios institucijai. Įgyvendinus šį reikalavimą pažeidimų identifikavimas būtų patikimesnis, nes centrinis subjektas disponuotų istoriniais skrydžių duomenimis, kurie, iškilus ginčui, teisėsaugos atstovams būtų prieinami. Turėdamos prieigą prie centrinės skrydžių duomenų bazės valdžios institucijos algoritmų pagalba taip pat galėtų nustatyti masinės stebėsenos apraiškų, kol šios neįgavo oportunistinio stebėjimo masto. Centralizuota nuotolinio identifikavimo sistema iš esmės remiasi pilotuojamų orlaivių oro eismo valdymo sistema. Tačiau joje orlaiviai identifikuojami ne nuotolinio identifikavimo priedais, o radarais. Šie buvo išrasti dar Antrojo pasaulinio karo metais[361]. Deja, šiuolaikinė radarų technologija nedidelių bepiločių orlaivių neatskiria nuo paukščių[362], todėl siekiant patikimo bepiločių identifikavimo ji šiuo metu nepanaudojama. Bepiločių orlaivių priedai, kurie internetu transliuotų skrydžio duomenis centrinei institucijai, leistų valdyti oro erdvę panašiu principu, kaip yra valdomas šiuolaikinių pilotuojamų orlaivių oro eismas. Disertacijos autoriaus nuomone, šiuo atveju nuotolinio identifikavimo priedai būtų ypač svarbi (jeigu ne pati svarbiausia) priemonė privatumo apsaugai užtikrinti.

Šiuo metu tokį pasiūlymą įgyvendinti tikriausiai būtų neįmanoma dėl nepakankamo technologinio išsivystymo. Iš esmės toks pats reikalavimas jau buvo numatytas pristatant pirminį JAV nuotolinių identifikavimo priedų reguliavimą. Buvo numatyta, jog bepilotis orlaivis turėtų nustatyto turinio duomenis transliuoti ne tik radijo ryšiu, bet ir internetu tiesiogiai (ne iš valdymo pulto, o iš paties bepiločio orlaivio) FAA paskirtam subjektui, kuris būtų kvalifikuotas teikti bepiločių orlaivių identifikavimo paslaugas. Siūlomas reguliavimas taip pat numatė, kad skleidžiamos žinutės elementai būtų viešai prieinami, bet galimybę susieti šią

359 Ishveena Singh, „This Free App Tracks Nearby Drone Flights Using Remote ID Data", *DroneDJ* (blog), 2022 m. spalio 4 d., https://dronedj.com/2022/10/04/remote-id-drone-tracking-app/ (tokias programėles jau galima parsisiųsti).

360 Žr. disertacijos 1.6 poskyrį.

361 Michael S. Nolan, *Fundamentals of air traffic control* (Cengage learning, 2011), 22.

362 Robin Radar Systems, „Why Traditional Radar Isn't Effective at Tracking Drones", žiūrėta 2022 m. gruodžio 19 d., https://www.robinradar.com/why-traditional-radar-isnt-effective-at-tracking-drones.

informaciją su bepiločių orlaivių registro duomenimis turėtų tik FAA ir teisėsaugos institucijos[363]. Tačiau galiausiai šio reikalavimo atsisakyta. Kaip teigia FAA, teisės akto derinimo su visuomene stadijoje buvo nustatyta daug techninių trūkumų, dėl kurių šiuo metu įgyvendinti tokį reikalavimą būtų sudėtinga[364]. Taigi įgyvendinti realiai veiksmingą centralizuotą nuotolinio identifikavimo sistemą šiuo metu neįmanoma dėl technologinių kliūčių.

Apibendrinant atliktą analizę galima teigti, kad iš pasirinktų jurisdikcijų detaliausiai nuotolinio identifikavimo priedų naudojimą yra reglamentavusios ES ir JAV. Jų taisyklės labai panašios. Tiek pagal ES, tiek pagal JAV reguliavimą bepiločiai orlaiviai turėtų vietiniu būdu per radijo ryšį transliuoti pagrindinius duomenis, leidžiančius susieti bepilotį orlaivį (jo valdytoją) su centralizuotu jų registru. Abiejų šalių reguliavimas turi trūkumų. ES taisyklės kritikuotinos dėl išimties, daromos nedideliems bepiločiams, kurių svoris nesiekia 250 g, šitai lemia, jog potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai nuotoliniu būdu būtų neatpažįstami nukentėjusiems tretiesiems asmenims. Disertacijos autorius šią problemą siūlo spręsti taip: privalomi nuotolinio identifikavimo priedai būtų privalomi tiktai bepiločiams, kurie geba rinkti asmens duomenis, arba tiesiog bepiločiams, kuriuos privaloma registuoti. JAV tam tikrą erdvę piktnaudžiauti gali atsirasti dėl „smėlio dėžių“ išimties, nes, kaip ir ES, potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai nuotoliniu būdu gali būti neatpažįstami nukentėjusiems tretiesiems asmenims. Vis dėlto piktnaudžiavimo tikimybę mažina griežtos JAV FAA taikomos baudos už taisyklių nesilaikymą. Piktnaudžiavimo galėtų padėti išvengti ir technologinis sprendimas. Gamintojus būtų galima įpareigoti bepiločius orlaivius iš anksto užprogramuoti taip, kad be kompetentingo subjekto leidimo jiems nepavyktų netgi pakilti zonose, kur tokiems bepiločiams orlaiviams vykdyti skrydžius draudžiama. Tiek JAV, tiek ES taisyklės turi esminį trūkumą, dėl kurio nuotolinio identifikavimo priedai šiuo metu nebūtų veiksminga privatumo apsaugos priemonė. Skrydžio identifikavimo duomenų transliavimas privalomas tik vietiniu būdu (radijo ryšiu), dėl to sunkiau nustatyti pažeidimus, kai stebėsena bepiločiais orlaiviais vykdoma slapta. Išeitis galėtų būti identifikavimo duomenų transliavimas ne tik radijo ryšiu, bet ir internetu centrinei valdžios institucijai. Vis dėlto, atsižvelgiant į pastarųjų metų JAV FAA patirtį, tokį pasiūlymą įgyvendinti būtų sudėtinga, nes šiuo metu nuotolinio identifikavimo technologijos nėra nepakankamai išsivystytos.

---

363 „Remote Identification of Unmanned Aircraft Systems“, Notice of proposed rulemaking, Federal Aviation Administration (FAA), FAA-2019-1100, 84 FR 72438, 2019 m. gruodžio 31 d.

364 „Remote Identification of Unmanned Aircraft“, Final rule, Federal Aviation Administration (FAA), FAA-2019-1100, 86 FR 4390, 2021 m. sausio 15 d.

2.3.8. Geografinio orientavimo funkcija

Geografinio orientavimo (angl. *geoawareness*) funkcija kartu su geografiniu apribojimu (angl. *geofencing*) galėtų sukurti virtualias kliūtis bepiločiams orlaiviams patekti į teritorijas, kurias juosia virtualus geografinis užtvaras, o žmonėms, esantiems ant žemės, galėtų suteikti galimybę realiu laiku valdyti bepiločių orlaivių skrydžius jų oro erdvėje, taip pat pasirinktinai juos riboti, kad teoriškai apsaugotų teritorinį asmenų privatumą. Jeigu bet kokių charakteristikų ir dydžių bepiločiai orlaiviai negalėtų prie pašalinių asmenų priartėti nepastebėti, daugelis privatumo pažeidimų, susijusių su bepiločiais, savaime išsispręstų. Siekiant įvertinti, ar dabartinis specialusis bepiločių orlaivių reguliavimas teikia tokių vilčių, vertėtų paanalizuoti geografinio orientavimo priedų taisykles. Privalomus geografinio orientavimo priedus šiuo metu numato tik JARUS ir ES reguliavimas. JAV šiuo metu tokio reikalavimo nėra, bet iš paruošiamųjų darbų matyti, kad ateityje tokių nuostatų tikriausiai atsiras. ICAO reguliavimas tokių priedų būtinumo nenumato.

JARUS geografinį orientavimą aiškina kaip „automatinę funkciją, kuri gali būti naudojama kaip patariamoji priemonė, padedanti orlaiviui neperžengti geografinių oro erdvės apribojimų“[365]. Reguliavimo tekste geografinio orientavimo funkcijai apibūdinti kaip sinonimas vartojamas geografinio apribojimo sistema. Pagal JARUS ji turėtų būti įrengta visuose bepiločiuose orlaiviuose, kurių svoris didesnis kaip 250 g. Išsamesnių techninių reikalavimų geografinio orientavimo priedams JARUS šaltiniai nenumato. Diskreciją nustatyti geografines zonų, kuriose būtų ribojami arba draudžiami bepiločių orlaivių skrydžiai ribas, JARUS palieka pačioms valstybėms nacionaliniu mastu[366].

ES geografinį orientavimą apibūdina kaip funkciją, „kuri, remdamasi valstybių narių pateiktais duomenimis, nustato galimą oro erdvės ribų pažeidimą ir įspėja nuotolinį pilotą, kad šis galėtų imtis veiksmingų veiksmų tam pažeidimui išvengti“[367]. Geografinio orientavimo priedai pagal ES reguliavimą privalomi visiems bepiločiams orlaiviams, išskyrus tuos, kurie sveria mažiau kaip 250 g (C0 klasė), aviamodelius (C4 klasė) ir privačiai sukonstruotus. Iš techninės pusės geografinio orientavimo priedai privalo: a) turėti sąsają duomenims su informacija apie oro erdvės ribas, susijusias su bepiločio orlaivio padėtimi ir aukščiu, nustatytas pagal geografines zonas, įkelti ir atnaujinti, užtikrinančią, kad nepablogėtų tų duomenų įvedimo arba atnaujinimo procesas ir nesumažėtų jų patikimumas; b) įspėti nuotolinį pilotą apie nustatytą galimą oro erdvės ribų pažeidimą; c) informuoti nuotolinį pilotą apie bepiločio orlaivio būklę ir įspėti, kai jo padėties nustatymo arba navigacijos sistemos negali užtikrinti tinkamo geografinio orientavimo

365 „Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, *supra note,* 273, 2 straipsnio 2 dalies l punktas.

366 *Ibid.*

367 Reglamentas (ES) 2019/945 3 straipsnio 32 punktas.

sistemos veikimo[368]. Nustatyti konkrečius ribojimus ir draudimus vykdyti skrydžius geografiškai apibrėžtose zonose ES reglamentavimas palieka valstybių narių kompetencijai[369].

JAV formalus reguliavimas šiuo metu privalomų geografinio orientavimo priedų nenumato, tačiau, kaip matyti iš FAA Bepiločių orlaivių patariamojo komiteto (DAC) rekomendacijų[370], toks reikalavimas gali atsirasti netolimoje ateityje. DAC vietoj geografinio orientavimo vartoja geografinio apribojimo terminą, kurį apibrėžia kaip būdą automatiškai apriboti bepiločių orlaivių patekimą į iš anksto nustatytą teritoriją (pvz., oro erdvę, esančią netoli jautrios vietos ar teritorijos). Vadovaujantis DAC rekomendacijomis, bepiločiai orlaiviai turėtų būti gaminami su geografinio apribojimo galimybe, nes tai vienas greičiausiai įgyvendinamų technologinių sprendimų, leisiančių sumažinti bepiločių orlaivių keliamas grėsmes saugumui[371]. Kaip švelnesnę alternatyvą geografiniam apribojimui DAC siūlo vykdyti automatizuotus bepiločių orlaivių skrydžių ribojimus. Jei geografinis apribojimas bepiločiams orlaiviams apskritai neleistų įskristi į tam tikrą teritoriją, tai taikant automatizuotą skrydžių apribojimą bepiločiam orlaiviui būtų leidžiama įskristi, bet ribojamas jo aukštis, greitis, manevringumas, nurodoma grįžti į paleidimo tašką ir pan. DAC rekomenduoja, kad prieš įskrendant į tokią zoną bepiločių orlaivių valdytojus reikėtų informuoti apie taikomus apribojimus[372].

Iš aptartų šaltinių matyti, kad geografinio orientavimo funkcijos reguliavimas tik pradinės stadijos. ES taisyklės yra tarsi detalesnė JARUS nuostatų versija, o apie JAV šiuo metu net neverta kalbėti, nes apie geografinio orientavimo funkcijos reikalingumą ten tik diskutuojama. Net ir ES taisyklės, iš visų analizuojamų jurisdikcijų išsamiausios (nors irgi lakoniškos), apsiriboja keliais abstrakčiais reikalavimais geografinio orientavimo priedams, o zonas, kuriose būtų ribojami skrydžiai bepiločiais orlaiviais, palieka nusistatyti pačioms valstybėms narėms. ES reguliavimas yra gan švelnus, t. y. geografinio orientavimo funkcija turėtų tik įspėti nuotolinį pilotą apie nustatytą galimą oro erdvės ribų pažeidimą, bet nedrausti skirsti į draudžiamas zonas. Tiesa, griežtesnius ir detalesnius reikalavimus gali nustatyti pačios valstybės narės. Kadangi iš specialiuose reguliavimo šaltiniuose randamų nuostatų sunku spręsti, ar įdiegta geografinio orientavimo sistema padėtų apsaugoti privatumą, galima tik padiskutuoti apie geografinio apribojimo ateitį bepiločių orlaivių kontekste.

Geografinio apribojimo technologija nėra nauja, ją jau naudoja daug kompanijų. Pvz., kai vartotojas patenka į geografiniu apribojimu apjuostą teritoriją,

---

368 Reglamentas (ES) 2019/945 priedo 2 dalies 13 punktas, 3 dalies 15 punktas, 4 dalies 10 punktas.

369 *Ibid.,* 15 straipsnis.

370 Drone Advisory Committee, *Drone Advisory Committee DAC Member eBook,* 2020, https://www.faa.gov/uas/programs_partnerships/drone_advisory_committee/media/Public_Ebook_v3a.pdf.

371 Drone Advisory Committee, 17.

372 *Ibid.,* 19.

socialinio tinklo programėlė jį gali paraginti apie tai paskelbti, ką nors nufotografuoti ar užmegzti virtualų pokalbį su netoliese esančiais draugais. Kai asmuo palieka šią teritoriją, jis gali būti paragintas palikti įvertinimą ar parašyti atsiliepimą. Geografinis apribojimas gali padėti darbdaviams sekti jų darbuotojų darbo laiką, pvz., darbuotojui atvykus į darbo vietą suaktyvinamas raginimas pranešti apie atvykimą iš savo mobiliojo prietaiso. Kai darbuotojas išeina iš darbo vietos, suaktyvinamas raginimas pranešti apie išvykimą. Geografinis apribojimas taip pat gali būti naudojamas asmeninėms reikmėms. Pvz., tokios programėlės kaip „FamiSafe" ar „Life360" leidžia tėvams nustatyti geografines užtvaras aplink savo ar auklės namus, vaiko mokyklą. Naudodamiesi šiomis programėlėmis, tėvai realiu laiku gali gauti perspėjimus kaskart jų vaikams įėjus ar išėjus iš apibrėžtos teritorijos[373]. Naudojama geografinio apribojimo technologija kelia rimtų grėsmių privatumui[374], nes iš geolokacinių duomenų galima nuspėti žmonių veiksmus, pomėgius, stebėti jų judėjimą erdvėje. Siekiant apsaugoti privatumą surinktus duomenis reikia anonimizuoti, tam yra kuriamos technologinės išeitys[375].

Vis dėlto grėsmės, kylančios privatumui, kai geografinio apribojimo technologija naudojama socialinių tinklų patirčiai pagerinti, marketingui, rinkodarai, darbuotojų ar vaikų stebėsenai, neaktualios kalbant apie bepiločius orlaivius. Pagrindinė geografinio apribojimo taikymo sritis, susijusi su bepiločiais orlaiviais, – tai zonos, kuriose nustatyti tam tikri draudimai ar apribojimai. Į tokias zonas įskridęs valdytojas iš karto gautų perspėjimą arba be atitinkamo asmens leidimo į jas įskristi ar jose pakilti negalėtų. Kalbant apie bepiločius orlaivius, tai būtų ne privatumą galinti pažeisti technologija, o atvirkščiai, – privatumą užtikrinti, nes jos pagrindinis tikslas būtų taikyti apribojimus bepiločių orlaivių skrydžiams, o ne rinkti duomenis apie jų skrydžius. Pvz., 2018 m. „Google" pateikė paraišką bepiločių orlaivių privatumo valdiklių patentui, kurio pagrindas yra būtent geografinio

373 „What Is Geofencing? Pros and Cons of Geofencing 2020", *TSheets,* žiūrėta 2020 m. lapkričio 17 d., https://www.tsheets.com/resources/geofencing-pros-cons.

374 Kearston L. Wesner, „Is the Grass Greener on the Other Side of the Geofence: The First Amendment and Privacy Implications of Unauthorized Smartphone Messages", *Case Western Reserve Journal of Law, Technology and the Internet* 10 (2019): [iii]-23; Ashley Thomas, „NO PLACE TO HIDE: Privacy Implications of Geolocation Tracking and Geofencing", *Scitech Lawyer* 16, 2 (2020): 20–23.

375 Jens Mathias Bohli ir kt., „PrivLoc: preventing location tracking in geofencing services", *International Conference on Trust and Trustworthy Computing* (Springer, 2014), 143–60; Mariana Cunha, Ricardo Mendes ir João P. Vilela, „Clustering Geo-Indistinguishability for Privacy of Continuous Location Traces", *2019 4th International Conference on Computing, Communications and Security (ICCCS)* (IEEE, 2019): 1–8; Christoph Bösch, „An Efficient Privacy-Preserving Outsourced Geofencing Service Using Bloom Filter", *2018 IEEE Vehicular Networking Conference (VNC)* (IEEE, 2018): 1–8; Ulrich Bareth, „Privacy-aware and energy-efficient geofencing through reverse cellular positioning", *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)* (IEEE, 2012): 153–58.

apribojimo technologija[376]. Kaip nurodoma patento paraiškoje, bepiločio orlaivio kompiuterio sistema gali būti sukonfigūruota taip, kad tam tikri jutikliai ar naudingosios apkrovos įrenginiai, prijungti prie bepiločio, būtų ribojami arba išjungiami priartėjus prie geografinio apribojimo zonos[377]. Duomenys apie bepiločio orlaivio skrydžio vietas taip pat būtų renkami ir profiliuojami, bet vien informacija apie tai, kur valdytojas vykdo skrydžius, mažai ką pasako apie jo privatų gyvenimą. Visgi asmenims, kurie gali būti sekami iš viršaus, galimybė sužinoti, kokiems subjektams priklausantys bepiločiai tądien skraidė prie jų geografinio apribojimo ar už jo ribų, gali reikšti galimybę apsaugoti savo privatumą.

Privatumo grėsmių būtų galima visiškai išvengti, jeigu kiekvienas asmuo naudodamasis geografiniu apribojimu pats valdytų, kuriems bepiločiams orlaiviams leidžiama skristi į jų oro erdvę, o kuriems – ne. Pvz., žmonės mobiliaisiais įrenginiais realiu laiku galėtų transliuoti, kad bepiločiai orlaiviai prie jų nesiartintų tam tikru atstumu arba kad praskrendantys bepiločiai automatiškai ištrintų ar paslėptų duomenis atsižvelgdami į nustatytas geografinio apribojimo ribas. Geografinio apribojimo technologijai pasiekus pakankamą interaktyvumo lygmenį ir pažangą, galimybės privatumui apsaugoti būtų praktiškai neribotos.

Ateityje, tikėtina, taip pat vertėtų judėti link reikalavimo taikyti privalomą geografinio orientacinio sistemos įdiegimą visiems bepiločiams orlaiviams, kurie turi jutiklius, galinčius fiksuoti asmens duomenis, nes šią taisyklę taikant tik didesnių gabaritų bepiločiams orlaiviams iš esmės paliekamas mikrodronų spiečius, galintis turėti dar didesnių galimybių pažeisti privatumą, nuošalėje.

Vertinant dabartinį specialųjį bepiločių orlaivių geografinių orientavimo funkcijos reguliavimą, disertacijos darbo autoriaus nuomone, dar anksti kalbėti apie tai, ar jis užtikrina pakankamą privatumo apsaugą, ar ne, nes jo nuostatos yra pernelyg abstrakčios. Tačiau kol geografinis apribojimas, taikomas bepiločiams orlaiviams, nėra gerai išvystytas, itin reglamentuoti šią sritį nereikėtų, kitaip būtų ribojama jos technologinė raida. Šiuo metu valstybės galėtų taikyti mažiau intervencinių priemonių, t. y. skatinti inovacijas, skirtas vystyti privatumą didinančias bepiločių orlaivių geografinio apribojimo technologijas (angl. *privacy-enhancing drone geofencing technologies*), pvz., informavimo reguliavimą, standartų kūrimą, taip pat ir ekonomines priemones – mokesčių lengvatas, kompensacijas ir pan.

Apibendrinant šį poskyrį, galima teigti, kad geografinis apribojimas yra didelį potencialą turinti, privatumą didinanti technologija bepiločių orlaivių srityje, ją taikant ateityje būtų galima išspręsti daugelį grėsmių, kylančių privatumui privačiose erdvėse (žemės sklypuose, namų erdvėje). Tačiau šiuo metu tiek geografinio apribojimo reguliavimas, tiek pati geografinio apribojimo technologija dar nėra pakankamai išvystyta. Siekiant skatinti šios inovacijos vystymąsi, disertacijos darbo autoriaus nuomone, valstybės turėtų imtis mažiau intervencinių priemonių,

376 Dana Livonia Contreras ir kt., Unmanned aerial vehicle privacy controls (*Google Patents,* issued 2018 m. sausio 25 d.).

377 *Ibid.,* 1.

kad būtų skatinamas jos panaudojimas privatumui apsaugoti nuo grėsmių, kurias kelia bepiločių orlaivių naudojimas.

2.3.9. Duomenų perdavimo ryšio linijos saugumo užtikrinimas

Reikalavimas apsaugoti nuo neteisėtos prieigos duomenų perdavimo ryšio liniją galėtų būti gera privatumo apsaugos priemonė. Kaip buvo minėta, saugumo neužtikrinimo pažeidimas bepiločių orlaivių kontekste gali pasireikšti trejopai: 1) įsilaužiant į bendras duomenų bazes, kurių apimtis didėja dėl bepiločių orlaivių naudojimo, 2) įsilaužiant į pačius bepiločius orlaivius, 3) bepiločius orlaivius naudojant kibernetiniams išpuoliams vykdyti. Duomenų ryšio linijos, palaikomos tarp valdymo pulto ir bepiločio orlaivio, apsauga nuo įsilaužimų galbūt didelės reikšmės neturėtų pirmai pažeidimų kategorijai, nes prie bendrų duomenų bazių prieinama įsilaužus į talpyklas, į kurias duomenys įvedami po skrydžių, visgi tai užkirstų kelią antros bei trečios kategorijos pažeidimams. Iš analizuojamų jurisdikcijų privalomą duomenų ryšio linijos saugumo užtikrinimą kai kuriems bepiločiams orlaiviams numato tik ES. Konkrečiai Reglamentas (ES) 2019/945 numato, kad C2 ir C3 klasės bepiločiuose orlaiviuose privalo būti įdiegta duomenų perdavimo ryšio linija, kuri būtų apsaugota nuo neteisėtos prieigos prie valdymo funkcijų[378]. JARUS yra nustačiusi techninius standartus, kurie turėtų padėti užtikrinti duomenų ryšio nenutrūkstamumą[379], tačiau juose neužsimenama apie perduodamos informacijos šifravimą, kuris būtų aktualus privatumo apsaugai.

Nors ES nuostata yra labai abstrakti, bet ji parodo privatumui svarbią bepiločių orlaivių reguliavimo kryptį. Tam, kad skrydžiai bepiločiais orlaiviais užtikrintų pakankamą privatumo apsaugą, duomenų ryšio linija privalo būti gana saugi. Ryšio linijos saugumo užtikrinti vien teisiniu reguliavimu neįmanoma, nes tai – techninis dalykas, priklausantis informacinių technologijų, inžinerijos sričiai, bet teisinis reguliavimas galėtų nurodyti bent jau šios technologijos vystymosi kryptį . ES reguliavimo nuostata tokią funkciją ir atlieka, ji nurodo, kad vienas iš bepiločių orlaivių integracijos kriterijų yra tinkamai apsaugota duomenų perdavimo ryšio linija.

Kita vertus, šios funkcijos nevertėtų sieti vien tik su bepiločio orlaivio dydžiu. C0 ir C1 klasės bepiločių orlaivių duomenų ryšio patikimumas, palyginti su didelio svorio bepiločiais orlaiviais, galbūt ne toks svarbus, kai kalbama apie ant žemės esančių žmonių sveikatos ir gyvybės apsaugą, bet ne mažiau svarbus, kai

---

378 Reglamentas (ES) 2019/945 priedo 3 dalies 8 punktas ir 4 dalies 12 punktas.

379 Joint Authorities for Rulemaking of Unmanned Systems, „Recommendations on the use of Controller Pilot Data Link Communications (CPDLC) in the RPAS communications context“, 2016 m. vasario 6 d.; Joint Authorities for Rulemaking of Unmanned Systems, „RPAS C2 link Required Communication Performance (C2 link RCP) concept“, 2014 m. spalio 10 d.; Joint Authorities for Rulemaking of Unmanned Systems, „Required C2 Performance (RLP) concept“, 2016 m. sausio 5 d.

kalbama apie ant žemės esančių žmonių sveikatos ir gyvybės apsaugą, bet ne mažiau svarbus, kai kalbama apie praeivių privatumo apsaugą. Mikrodronų spiečiai ar nedideli bepiločiai orlaiviai gali turėti netgi žymiai platesnes galimybes pažeisti privatumą negu dideli, todėl taip pat svarbu yra užtikrinti, kad jų duomenų ryšys nebūtų neteisėtai užgrobtas.

Pažymėtina, kad dėl nesaugaus duomenų ryšio tarp bepiločio orlaivio ir valdymo pulto daugelis kitų privatumo apsaugos priemonių gali būti neveiksmingos. Pvz., bepiločių orlaivių ar jų valdytojų registracija, identifikavimo funkcija negalėtų padėti nustatant pažeidimą įvykdžiusio asmens tapatybę, jeigu jį atliktų ne teisėtas bepiločio orlaivio valdytojas, o neteisėtai jį užgrobęs tretysis asmuo.

Taip pat akcentuotina, kad dabartinis ES reguliavimas, nors ir nustato kryptis duomenų ryšio kibernetiniam saugumui, bet to gali nepakakti, kad gamintojai savireguliacijos būdu sukurtų patikimas duomenų ryšio apsaugos technologijas. Manytina, jog duomenų ryšio šifravimas (angl. *C2 link encryption*) yra viena pagrindinių privatumo apsaugą galėsiančių užtikrinti technologijų, todėl valstybės konsultuodamosis su gamintojais ir nevyriausybinėmis organizacijomis turėtų rasti tarptautinį konsensusą dėl patikimiausių būdų apsaugoti kiekvienos kategorijos skrydžių duomenų ryšio liniją.

Taigi, duomenų perdavimo ryšio linijos saugumo užtikrinimas yra svarbi užduotis norint sukurti tvarų bepiločių orlaivių reguliavimą, kuriame būtų skiriama pakankamai dėmesio žmonių privatumo apsaugai. Nors duomenų ryšio šifravimo technologijos vystymasis priklauso nuo informacinių technologijų ir inžinerijos mokslininkų pastangų, tačiau teisinis reguliavimas galėtų apibrėžti šios inovacijos vystymosi kryptį. Šalys turėtų skirti dėmesį ne tik tam, kad duomenų ryšys būtų nepertraukiamas, bet ir tam, kad būtų užtikrintas jo saugumas.

2.3.10. Reikalavimas gaminti bepiločius orlaivius su žibintais

Prie bepiločio orlaivio pritaisyti mirksintys žibintai gali ne tik pagelbėti VLOS skrydį vykdančiam valdytojui stebėti jo judėjimo trajektoriją ar kitiems oro erdvės dalyviams pamatyti bepilotį orlaivį nakties metu, bet ir padėti atkreipti aplinkinių dėmesį, kad oro erdvėje netoli jų pakibęs asmens duomenis galintis rinkti bepilotis. Vertėtų aptarti, kaip šį reikalavimą įgyvendina analizuojamų jurisdikcijų reguliavimas. Reikalavimus turėti prie bepiločio orlaivio žibintus numato tik ES ir JAV reguliavimas, o ICAO ir JARUS rekomendacijose tokių taisyklių nėra.

ES privalomų žibintų nenumato tik C0 klasės bepiločiams orlaiviams, o visi kiti privalo turėti šviesos šaltinį, kuris padėtų nuotoliniam pilotui bepilotį orlaivį valdyti ir leistų ant žemės esantiems žmonėms jį atskirti nuo pilotuojamų orlaivių[380].

380 Reglamentas (ES) 2019/947 priedo 2 dalies 16 punktas, 3 dalies 18 punktas, 4 dalies 14 punktas.

JAV bepiločiai orlaiviai privalo turėti žibintus tik tada, jeigu planuojama skrydį vykdyti prieblandoje. Tokiu atveju žibinto skleidžiama šviesa turėtų būti matoma iš mažiausiai 3 mylių atstumo[381]. Nakties metu skrydžiai šiuo metu draudžiami[382], bet juos planuojama legalizuoti numatant, kad nakties metu bepilotis turėtų skleisti šviesą, matomą bent iš 3 mylių[383].

Kaip matyti iš aptartų nuostatų, ES ir JAV požiūris į bepiločių orlaivių žibintus skirtingas. ES labiau laikosi požiūrio, kad beveik visi bepiločiai orlaiviai turėtų turėti žibintus, nėra svarbu, kokiu paros metu vykdomi skrydžiai, – vien tam, kad skleidžiama šviesa padėtų nuotoliniam pilotui jį valdyti. JAV laikosi požiūrio, kad žibintai turėtų būti privalomi tik tamsiuoju paros metu arba prieblandoje. Akivaizdu, jog privatumo apsaugai palankesnis ES požiūris. Tačiau žibintai dėl nedidelės įrengimo kainos, manytina, turėtų būti privalomi visų rūšių bepiločiams orlaiviams, nepriklausomai nuo jų svorio. Pagal ES reguliavimą, kaip jau buvo minėta, bepiločių orlaivių valdytojų registracija būtina tais atvejais, jeigu skrydis vykdomas bepiločiu orlaiviu, turinčiu jutiklius, kurie fiksuoja asmens duomenis. Tačiau bepiločiai, sveriantys mažiau kaip 250 g, tokius jutiklius turi, net ir registruoti viešame registre, nors ir su nuotolinio identifikavimo priedais (pagal dabartinį ES reguliavimą tokiems bepiločiams orlaiviams neprivalomi nuotolinio identifikavimo priedai) galėtų būti visiškai nepastebimi pašaliniams asmenims, jeigu neturėtų žibintų, ypač jeigu kalbame apie mikrodronų spiečius. Kitaip tariant, ant žemės esantis asmuo, neatkreipęs dėmesio į ore kybantį bepilotį orlaivį (ar jų spiečius) ir nepasidomėjęs savo išmaniajame įrenginyje, ar netoliese nėra jį stebinčių bepiločių orlaivių, galėtų net nežinoti apie vykdomą privatumo pažeidimą jo atžvilgiu.

Taigi, žibintai yra viena lengviausiai įgyvendinamų, pigiausių ir itin veiksmingų priemonių, kurios galėtų apsaugoti privatumą. Todėl reikalavimas gaminti bepiločius orlaivius su žibintais turėtų būti taikomas visiems bepiločiams, galintiems fiksuoti asmens duomenis, nepriklausomai nuo to, ar skrydis vykdomas dienos, ar nakties metu. Bepiločių orlaivių šviesos šaltinis turėtų būti tokio stiprumo, kad būtų matomas iš atstumo, kuris veiksmingai apsaugotų privatumą ir atkreiptų pašalinių asmenų dėmesį netgi saulėtą dieną.

2.4. Skyriaus išvados ir rekomendacijos

Apibendrinant specialiųjų bepiločių orlaivių reguliavimo šaltinių analizę, apie kiekvieną iš hipotetinių privatumo apsaugos priemonių galima daryti tokias išvadas:

381 JAV CFR 14 antraštės 107.29 straipsnio b punktas.

382 *Ibid.,* a punktas.

383 Federal Aviation Administration, „Operation of Small Unmanned Aircraft Systems Over People“, Docket No.: FAA–2018–1087 § (2019), https://www.federalregister.gov/documents/2019/02/13/2019-00732/operation-of-small-unmanned-aircraft-systems-over-people.

Reikalavimas laikytis atstumo taip, kaip jį pateikia dabartinės taisyklės, nebūtų pakankama privatumo apsaugos priemonė. Dabartinis bepiločių orlaivių reguliavimas šią pareigą aptaria trejopai: 1) ICAO ir ES nurodo konkrečius atstumus, kurių privalo laikytis bepilotis orlaivis nuo pašalinių asmenų, 2) JARUS numato bendrą pareigą laikytis saugaus atstumo, 3) JAV konkretus atstumas nenumatytas. Disertacijos autoriaus nuomone, veiksmingas reguliavimas galėtų būti toks, kuris numato konkretų atstumą, tačiau ir tai tebūtų trumpalaikė ir netiesioginė privatumo apsaugos priemonė nuo bepiločių, kurių vaizdo kamera nepasižymi labai aukšta raiška, o mikrofonai dideliu pažangumu. Siekiant tiksliai nustatyti atstumą, apsaugantį asmenų privatumą nuo bepiločių orlaivių, reikėtų kiekvieną situaciją vertinti individualiai, o tai labai padidintų laiko sąnaudas. Taigi tokia priemonė nėra veiksminga apsaugoti nuo privatumo grėsmių, kylančių dėl bepiločių orlaivių naudojimo.

Reikalavimas informuoti (gauti sutikimą) taip, kaip yra pateiktas dabartinėse taisyklėse, nebūtų veiksmingas būdas privatumui apsaugoti. Pirmiausia dėl informavimo (norint gauti sutikimą) sudėtingumo. Skrydžių bepiločiais orlaiviais negalima prilyginti naršymui internete, kur informavimo (sutikimo) procedūra naudojama plačiausiai. Internetinėje erdvėje sutikimo galima paprašyti prieš asmeniui pradedant naudotis tinklalapiu, o šiam nesutikus, tinklalapis gali automatiškai išsijungti arba tiesiog nerinkti duomenų apie lankytoją. Tačiau realiame pasaulyje yra sunku įsivaizduoti mechanizmą, kuris visus žmones, esančius bepiločio orlaivio skrydžio teritorijoje, automatiškai informuotų apie planuojamą skrydį, o jei jie nesutiktų, duomenų nerinktų. Šią keblią situaciją ICAO sprendžia itin sumažindama reikalavimus, keliamus sutikimui gauti, – taigi sutikimas gali būti numanomas, o dėl tokio reglamentavimo bepiločių orlaivių valdytojams sudaroma galimybė piktnaudžiauti. ES reikalavimai sutikimui labai griežti ir išsamūs, tačiau praktiškai neįgyvendinami vykdant skrydžius ten, kur yra didesni žmonių susibūrimai. JAV laikomasi požiūrio, kad šiuo metu formaliai nustatyti reikalavimą informuoti ir gauti aplinkinių sutikimą nėra reikalo, tai tik rekomenduojama ir tik tada, kai pats bepiločio orlaivio valdytojas mano, kad gali įsibrauti į kažkieno asmeninę erdvę.

Registracijos reikalavimas yra viena svarbiausių privatumo apsaugos priemonių, užtikrinančių asmenų galimybę įgyvendinti teisę kreiptis į teismą teisminės gynybos, tačiau šį reikalavimą tinkamai įgyvendina ne visos analizuojamos jurisdikcijos. Šio reikalavimo išimtys, kurių taikymas priklauso vien nuo bepiločio orlaivio svorio (JARUS), gamintojams sudaro galimybes gaminti už teisės ribų išeinančius, bet privatumą tiek pat galinčius pažeisti bepiločius orlaivius. Registruoti visus bepiločius (ICAO, JAV) yra geriau, nei numatyti svorio apribojimą, bet irgi ne pats geriausias variantas, nes gali būti ribojamas bepiločių orlaivių kaip žaislų naudojimas. Visgi nuostatos, numatančios ne tik svorio apribojimus, bet ir papildomas sąlygas, pvz., bepilotis negali fiksuoti asmens duomenų arba yra žaislas (ES), turėtų pasiteisinti ir galėtų būti gerosios praktikos pavyzdžiu kitų valstybių teisiniam reguliavimui.

Reikalavimas kaupti įrašus padėtų užtikrinant tam tikrą privatumo apsaugą, tačiau dabartiniuose specialiuose bepiločių orlaivių reguliavimo šaltiniuose kaupiamų duomenų apimtis yra per siaura, kad privalomas duomenų kaupimas būtų veiksminga privatumo apsaugos priemonė. Aukštesnį apsaugos lygį galėtų užtikrinti daugiau kaupiamų duomenų, tačiau tiktai tokiu atveju: 1) jeigu šie duomenys būtų tik pačiame bepilotyje orlaivyje, nebūtų prieinami internetu, 2) tretiesiems asmenims būtų teikiami tik pagal teisėtą įgaliotos valdžios institucijos (teismo, ikiteisminio tyrimo pareigūno ar kt.) pareikalavimą, 3) turėtų konkretų ribotą saugojimo terminą.

Kvalifikacijos reikalavimus bepiločių orlaivių pilotams numato tik dvi iš analizuotų jurisdikcijų (JARUS ir ES). Reikalavimai prie įsigyjamo bepiločio orlaivio pridėti naudotojo vadovą, rengti informacines kampanijas, didesnių pajėgumų bepiločių orlaivių valdytojus įpareigoti baigti specialius mokymus ir taikyti sankcijas už išsilavinimo reikalavimų nesilaikymą gali būti veiksmingos privatumo apsaugos priemonės, tačiau jų įgyvendinimas neturėtų būti formalus. Gamintojo vadovuose ir privalomuose mokymuose pateikiama informacija turėtų būti įsimintina, tikslinga ir praktiška, kad prisidėtų prie privatumo apsaugos. Informacinės kampanijos turėtų būti skirtos kuo siauresnei auditorijai, rengiami patrauklūs pranešimai, raginantys veikti ir įvardijantys, ką konkrečiai reikėtų keisti.

Reikalavimai atlikti rizikos vertinimą pagal dabartinį specialųjį bepiločių orlaivių reguliavimą vargu ar galėtų suteikti tinkamą privatumo apsaugą, nes juo vadovaujantis operatoriai neprivalo įvertinti rizikos privatumui, kurią gali kelti vykdomas skrydis. Vis dėlto rizikos vertinimas, kaip priemonė, galėtų būti veiksminga privatumui apsaugoti, jeigu prieš tam tikrus skrydžius operatoriai būtų įpareigoti įvertinti ir galimą žalą privatumui. Tokią priemonę numato ES duomenų apsaugos teisės aktai.

Nuotolinio identifikavimo priedus iš pasirinktų jurisdikcijų detaliausiai yra reglamentavusios ES ir JAV. Jų taisyklės labai panašios. Tiek pagal ES, tiek pagal JAV reguliavimą bepiločiai orlaiviai turėtų vietiniu radijo ryšiu transliuoti pagrindinius duomenis, leidžiančius susieti bepilotį orlaivį (jo valdytoją) su centralizuotu registru. Abiejų šalių reguliavimas turi tam tikrų trūkumų. ES taisyklėse kritikuotina išimtis, daroma nedideliems bepiločiams, sveriantiems mažiau nei 250 g; dėl šios išimties potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai nuotoliniu būdu būtų neatpažįstami nukentėjusiems tretiesiems asmenims. Šią problemą disertacijos autorius siūlo spręsti siejant nuotolinio identifikavimo priedų privalomumą su gebėjimu rinkti asmens duomenis arba tiesiog su registracijos reikalavimu. JAV tam tikra erdvė piktnaudžiavimui gali atsirasti dėl „smėlio dėžių“ išimties, dėl jos kyla ta pati problema, kaip ir ES, – potencialiai privatumą galintys pažeisti nedideli bepiločiai orlaiviai nuotoliniu būdu gali būti neatpažįstami nukentėjusiems tretiesiems asmenims. Vis dėlto piktnaudžiavimo tikimybę mažina griežtos JAV FAA baudos už taisyklių nesilaikymą. Disertacijos autoriaus nuomone, technologinė išeitis taip pat galėtų padėti išvengti piktnaudžiavimo. Bepiločių gamintojai galėtų būti įpareigoti bepiločius orlaivius iš anksto

užprogramuoti taip, kad be kompetentingo subjekto leidimo nepavyktų netgi pakilti zonose, kur tokiems bepiločiams orlaiviams vykdyti skrydžius draudžiama. Tiek JAV, tiek ES taisyklės turi esminį trūkumą, dėl kurio nuotolinio identifikavimo priedai nebūtų veiksminga privatumo apsaugos priemonė. Skrydžio identifikavimo duomenų transliavimas dabar privalomas tik vietiniu būdu (radijo ryšiu), o tai apsunkina pažeidimų nustatymą, kai bepiločiais orlaiviais vykdoma slapta stebėsena. Išeitis galėtų būti identifikavimo duomenų transliavimas ne tik radijo ryšiu, bet ir internetu centrinei valdžios institucijai. Tačiau tokį pasiūlymą, sprendžiant iš pastarųjų metų JAV FAA požiūrio, įgyvendinti būtų sudėtinga dėl nepakankamai išvystytos nuotolinio identifikavimo technologijos.

Geografinio orientavimo (arba geografinio apribojimo) funkcija yra didelį potencialą turinti, privatumą didinanti technologija bepiločių orlaivių srityje, ją naudojant ateityje būtų galima išspręsti daugelį bepiločių orlaivių keliamų grėsmių privatumui privačiose erdvėse (žemės sklypuose, namų aplinkoje). Tačiau šiuo metu tiek geografinio apribojimo reguliavimas, tiek geografinio apribojimo technologija dar nėra gerai išvystyta. Siekiant skatinti šios inovacijos vystymąsi, disertacijos darbo autoriaus nuomone, valstybės turėtų imtis mažiau intervencinių priemonių, kad būtų skatinamas jos pritaikymas privatumui apsaugoti nuo grėsmių, kylančių dėl bepiločių orlaivių naudojimo.

Duomenų perdavimo ryšio linijos saugumo užtikrinimas yra svarbi užduotis norint sukurti tvarų bepiločių orlaivių reguliavimą, kuriame būtų skiriama pakankamai dėmesio žmonių privatumo apsaugai. Nors duomenų ryšio šifravimo technologijos vystymasis priklauso nuo informacinių technologijų ir inžinerijos mokslininkų pastangų, bet teisinis reguliavimas galėtų nurodyti šios inovacijos vystymosi kryptį. Manytina, kad šalys turėtų skirti dėmesį ne tik nepertraukiamam duomenų ryšiui, bet ir jo saugumui užtikrinti.

Reikalavimas bepiločius orlaivius gaminti su žibintais yra viena lengviausiai įgyvendinamų, pigiausių ir veiksmingiausių priemonių, galinti apsaugoti privatumą. Todėl šis reikalavimas turėtų būti taikomas visiems bepiločiams orlaiviams, galintiems fiksuoti asmens duomenis, nepriklausomai nuo to, ar skrydis vykdomas dienos, ar nakties metu. Be abejo, bepiločių orlaivių šviesos šaltinis turėtų būti atitinkamo stiprumo, kad būtų matomas bent jau iš atstumo, kuris galėtų būti veiksmingas apsaugant privatumą, ir atkreiptų pašalinių asmenų dėmesį net ir saulėtą dieną.

Kaip matyti iš atlikto specialiųjų bepiločių orlaivių reguliavimo šaltinių tyrimo, šio skyriaus pradžioje iškelta hipotezė pasitvirtino, nes visos aptartos priemonės vienokiu ar kitokiu būdu galėtų užkirsti kelią privatumo pažeidimams. Vis dėlto šiuo metu privatumo pažeidimų prevencijos daugelis išvardytų priemonių realiai neužtikrina, nes jas reglamentuojančios nuostatos turi trūkumų, kai kurios jų dar nėra iki galo įgyvendintos arba jas įgyvendinti būtų sunku. Tačiau, nepaisant specialiojo bepiločių orlaivių reguliavimo trūkumų, pamatai bepiločių orlaivių nepastebimumui mažinti jau yra padėti ir reikia tikėtis, jog kartu su privatumą didinančių technologijų pažanga tobulės ir prevencinių privatumo apsaugos priemonių reglamentavimas.

3. BEPILOČIAI ORLAIVIAI IR PRIVATUMAS VIEŠOJOJE ERDVĖJE

Detaliai aptarus privatumo apsaugos priemones, kurias numato specialusis bepiločių orlaivių reguliavimas, vertėtų paanalizuoti, kokias išeitis siūlo bendras privatumo reguliavimas. Kaip jau minėta, vienas iš pažeidimų, kuriuos gali sukelti nedidelių bepiločių orlaivių naudojimas, yra stebėsena[384]. Galima teigti, jog bepiločių orlaivių kontekste ši pažeidimo rūšis turi bene didžiausią reikšmę, nes įgalina oportunistinį, visur esantį informacijos rinkimą, o tai savo ruožtu sukelia kitų privatumo pažeidimų[385]. Tokio pobūdžio informaciją lengviausia ir aktualiausia būtų rinkti viešojoje erdvėje, todėl vienas iš būdų ieškoti išeičių daugumai grėsmių, kylančių privatumui dėl vis plačiau naudojamų bepiločių orlaivių, yra per vieną iš teisės į privatų gyvenimą ribojimo pagrindų – kai duomenys renkami viešoje vietoje. Apie tai bus šis disertacijos skyrius, įgyvendinantis ketvirtąjį uždavinį. Skyrių sudaro keturi poskyriai. Pirmajame aptariama privatumo viešojoje erdvėje problematika. Antrajame ieškoma teorinių privatumo reguliavimo viešojoje erdvėje išeičių moksliniame diskurse. Trečiame poskyryje analizuojama EŽTT ir Lietuvos teismų taikoma praktika, kai sprendžiami klausimai, susiję su privatumu viešojoje erdvėje, ir diskutuojama, kaip galima pritaikyti jurisprudencijos taisykles ir bepiločiams orlaiviams. Paskutiniame poskyryje apibendrinami privatumo apsaugos sprendimai, nagrinėti šiame disertacijos skyriuje.

Tyrimo apribojimai ir analizės ribos

Atliekant tyrimą šioje disertacijos dalyje buvo būtina nustatyti jo ribas ir pasirinkti analitinius prioritetus, leidžiančius išlaikyti disertacijos kryptingumą bei užtikrinti gautų rezultatų aktualumą. Vienas iš tokių metodologinių sprendimų buvo riboti analizuojamą jurisprudenciją ir koncentruotis į teisines sistemas, kurios yra tiesiogiai susijusios su Lietuvos teismų praktika ir galimu būsimo reguliavimo kontekstu.

Atsižvelgiant į tai, kad antroje disertacijos dalyje buvo išsamiai analizuojami tiek Europos Sąjungos, tiek Jungtinių Amerikos Valstijų specialieji bepiločių orlaivių reguliavimo šaltiniai, sistemiška būtų šiame skyriuje nagrinėti ir JAV teismų praktiką privatumo viešojoje erdvėje kontekste. Tačiau sąmoningai pasirinkta jos neanalizuoti, nes JAV privatumo teisė remiasi iš esmės kitokia metodologija nei Europos teisinė sistema, o ten suformuoti teisės aiškinimo standartai yra sunkiai tiesiogiai pritaikomi Lietuvos teismų praktikoje.

JAV teisminėje praktikoje vyrauja dvinarė privatumo samprata, kurioje griežtai atribojamos viešoji ir privati erdvė – privatumo apsauga taikoma beveik išimtinai privačioje erdvėje, o teisėti lūkesčiai dėl privatumo viešoje vietoje paprastai yra labai riboti. Šis požiūris esmingai skiriasi nuo Europos žmogaus teisių konvencijos

384 Stebėsena suprantama kaip žiūrėjimas, klausymasis arba įrašymas to, ką asmuo veikia. Žr. disertacijos 1.5.1 poskyrį.

385 Žr. disertacijos 1 skyrių.

(EŽTK) 8 straipsnio aiškinimo Europos Žmogaus Teisių Teismo (EŽTT) jurisprudencijoje, kurioje pripažįstama, kad asmuo gali tikėtis tam tikro privatumo net ir viešojoje erdvėje, ypač kai stebėsena yra sisteminė, ilgalaikė arba vykdoma pasitelkiant modernias technologijas. Lietuvos teismų praktika daug labiau remiasi EŽTT suformuotais privatumo standartais, todėl JAV jurisprudencijos analizė nepridėtų reikšmingos pridėtinės vertės šiam tyrimui.

Siekiant išlaikyti analitinį nuoseklumą ir išvengti perteklinės informacijos, analogiškai buvo priimtas sprendimas atrinkti tik tas bylas, kurios geriausiai atskleidžia aktualias teisines problemas privatumo viešojoje erdvėje kontekste. Nors tyrimo metu buvo išanalizuota platesnė jurisprudencijos apimtis, įskaitant ir Lietuvos vyriausiojo administracinio teismo (LVAT) praktiką, šiame disertacijos skyriuje šio teismo bylos neaptariamos. Toks sprendimas priimtas atsižvelgiant į tai, kad nebuvo identifikuota nė viena byla, kurios faktinės aplinkybės ar teisiniai argumentai būtų tiesiogiai susiję su privatumo apsaugos viešojoje erdvėje problematika bepiločių orlaivių kontekste. Todėl, siekiant išvengti perteklinės informacijos ir išlaikyti tyrimo fokusą, ši jurisprudencija detaliai neanalizuojama.

Kadangi pagrindinis dėmesys buvo skiriamas privatumo apsaugai bepiločių orlaivių naudojimo sąlygomis, pirmenybė teikta išsamiai bylų analizei, o ne kiekybinei jų apžvalgai. Toks tyrimo metodologijos pasirinkimas ne tik padeda aiškiau identifikuoti esminius jurisprudencijos principus, bet ir leidžia formuluoti pagrįstas rekomendacijas būsimam teisminiam aiškinimui bei teisėkūros procesui Lietuvos teisinėje sistemoje.

3.1. Privatumo viešoje vietoje problematika

Nors tai, kas vyksta už uždarų durų namų erdvėje, priskiriama privačiam gyvenimui ir laikoma, kad jos stebėjimas bepiločiu orlaiviu būtų privatumo pažeidimas. Visai kas kita apibrėžti teisės į privatumą ribas, kai stebėjimas vyksta viešojoje erdvėje. Kaip jau minėta pirmame skyriuje, viešojoje erdvėje skraidantys bepiločiai gali neigiamai paveikti individų laisvės pojūtį, kūrybingumą, saviugdą, priversti jaustis nepatogiai, sukelti elgesio pakitimų, net jeigu bepiločiai orlaiviai neįžiūrimi plika akimi ar negirdimi[386].

Tai būtų galima iliustruoti pateikiant hipotetinę situaciją iš netolimos ateities, tarkim, vartotojų elgsenos tyrimais užsiimanti konsultavimo bendrovė, norėdama dar tikslesnių spėjimų ir taip padidinti pelną, nusprendžia išbandyti bepiločių orlaivių technologiją. Bendrovė nusiperka kelis tūkstančius naujausios technologijos vabzdžio dydžio bepiločių orlaivių, kurie gali vykdyti stebėjimą iš arti, ir keliasdešimt fiksuotų sparnų „motininių“ bepiločių. Atliekant elgsenos tyrimus bepiločiai orlaiviai užprogramuojami viešojoje erdvėje atpažinti ir sekti tam tikras individų grupes, pvz., jeigu užsakovą domina jaunų darbingų žmonių įpročiai arba pokalbių temos, bepiločių spiečiui duodama komanda sekti, klausytis

386 *Ibid.*

individų, kurių amžius yra 20–30 metų. Surinktus duomenis bendrovė įveda į savo duomenų bazes ir derina su jau turimais elektroniniais individų profiliais, apie kuriuos informaciją nusipirko iš duomenų valdytojų internete.

Nors pateiktame pavyzdyje stebėjimas vyksta viešosiose erdvėse, visgi kiekvienas nujaučiame, kad netgi būdami vietose, kur mus supa daug žmonių, ne viską norėtume atskleisti aplinkiniams. Tačiau kai bandome apibrėžti, kur baigiasi privatumo ribos viešoje vietoje, pasidaro sudėtingiau. Žmonės natūraliai jaučiasi nejaukiai, kai kažkas slapta renka informaciją apie juos, bet ar tai reiškia, kad visus skrydžius bepiločiais orlaiviais viešoje vietoje reikėtų uždrausti saugant privatumą? Disertacijos autoriaus vertinimu, vien dėl to, kad yra nepamatuota tikimybė, jog bus pažeistas aplinkinių žmonių privatumas, visiškai uždrausti bepiločių orlaivių skrydžius nebūtų tinkamas sprendimas, reikėtų apsibrėžti ribas. Tokių santykių galima būtų ir visiškai nereguliuoti, o leisti apibrėžti ribas teismams ir pačiai rinkai. Tačiau ir šiuo atveju reikėtų teorinio pagrindo, kuris leistų teismams ar bepiločių orlaivių rinkos suinteresuotoms šalims laikytis nuoseklios vertybinės krypties. Apie privatumą viešoje erdvėje aktyviausiai diskutuoja JAV mokslininkai, iš jų vertėtų išskirti tris autorius: H. Nissenbaum, J. Reidenbergą ir M. E. Kaminski.

3.2. Teorinis pagrindas reguliuojant privatumą viešojoje erdvėje

3.2.1. Kontekstinio integralumo teorija

Vienas iš būdų analizuoti grėsmes privatumui viešoje erdvėje yra per grėsmes, susijusias su surinktų duomenų panaudojimu. Rašydama apie privatumą viešojoje erdvėje H. Nissenbaum nurodo, kad tradicinės privatumo teorijos orientuojasi į privačios ir viešosios erdvės dichotomiją, tvirtindamos, jog privatumas gali būti pažeistas tik tada, kai atskleidžiami privačioje erdvėje surinkti arba privatūs asmens duomenys. Tačiau pagal jos teoriją, kurią ji vadina „kontekstiniu integralumu“, svarbu ne tai, kokioje erdvėje (viešojoje ar privačioje) buvo surinkti duomenys, o kokiame kontekste jie buvo surinkti[387].

Viešosios ir privačios erdvės dichotomijos trūkumas tas, kad kai informacija yra atskleidžiama viešai, ji neva praranda visas pretenzijas į privatumą. Vis dėlto, pasak H. Nissenbaum, netgi informacija, kurią žmogus sąmoningai apie save atskleidžia viešojoje erdvėje, neturėtų būti suprantama, kaip tokia, kurią galima naudoti be asmens sutikimo ir be jokių apribojimų. Asmuo gali atskleisti tam tikrą informaciją viename viešosios erdvės kontekste, nes tikisi, jog ši niekada tos aplinkos nepaliks, o kitame kontekste tą pačią informaciją gali norėti laikyti privačia. H. Nissenbaum teigia, kad grėsmė privatumui kyla, kai informacija būna paimta iš vieno konteksto ir perkelta į kitą aplinką, nepaisant aplinkybių, kurios asmeniui leidžia manyti, kad ta pati informacija tarp šių vietų neturės galimybės judėti[388].

---

387 Helen Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life* (Stanford University Press, 2009).

388 *Ibid.,* 233.

Ferdinandas Shoemanas šią problemą iliustruoja tokiu pavyzdžiu: asmuo gali būti aktyvus homoseksualų judėjimo dalyvis San Fransiske, bet nenori atskleisti savo seksualinių pažiūrų šeimos nariams ar kolegoms Sakramente. Universiteto profesorius gali būti dažnas lankytojas ir kitiems homoseksualams gerai pažįstama persona vietiniame gėjų bare, tačiau universitete jis gali nenorėti atskleisti savo seksualinės orientacijos. Be abejo, San Fransisko gatvės ir laikraščiai yra viešos vietos, kaip ir gėjų barai ramiame universiteto miestelyje[389]. Tačiau tai, jog asmuo kai kuriose viešose vietose pasirodė kaip gėjų aktyvistas, nebūtinai reiškia, kad jis visam pasauliui viešai pareiškė esantis homoseksualių pažiūrų ir kad šią informaciją turėtų žinoti jo kolegos bei šeimos nariai.

H. Nissenbaum pasiūlytas privačios informacijos charakterizavimas pagal kontekstą yra įtakinga teorija, dažnai pateikiama kaip alternatyva dvinarei, arba dichotominei, privatumo teorijai[390]. Kai kurie autoriai įžvelgia kontekstinio integralumo teorijos panašumus su BDAR 89 straipsnio 1 dalyje[391] įtvirtintam tikslo apribojimo principui ir mano, jog ši teisės norma kilo būtent iš H. Nissenbaum teorijos[392].

Toliau vertėtų panagrinėti, ar kontekstinio integralumo teorija yra tinkamas įrankis, kuriuo įstatymų leidėjai galėtų naudotis kurdami įstatymus, apsaugančius nuo bepiločių orlaivių keliamų grėsmių privatumui, o teismai – spręsdami su bepiločiais orlaiviais susijusias bylas. Kaip jau minėta ankstesniame disertacijos skyriuje, bepiločiais orlaiviais galima sukelti privatumo pažeidimus tiesiogiai, naudojantis jais kaip informacijos rinkimo priemone (stebėsena) arba informacijos platinimo priemone (atidengimas), taip pat ir netiesiogiai – kaip informacijos apdorojimo įrankiu (agregavimas, identifikavimas, saugumo neužtikrinimas), kuris tiesiog padidina duomenų iš realaus pasaulio prieinamumą[393]. Kitaip tariant, bepiločiai orlaiviai dalyvaudami renkant duomenis prisideda prie tokių pažeidimų kaip agregavimas, identifikavimas ir saugumo neužtikrinimas, tačiau šie pažeidimai nekyla tiesiogiai iš jų naudojimo.

Kontekstinio integralumo teorija pabrėžia grėsmes, atsirandančias dėl duomenų perkėlimo iš vieno konteksto į kitą, surinktų duomenų lyginimo tarpusavyje siekiant nustatyti elgesio šablonus visuomenėje, tačiau patį duomenų rinkimą viešoje vietoje palieka nuošalėje. Kitaip tariant, Nissenbaum privatumo viešojoje erdvėje reguliavimo modeliu pagrindžiama, kodėl į viešąją erdvę patekę duomenys neturėtų būti perkeliami iš vieno konteksto į kitą ar kitaip manipuliuojami, tačiau

389 Ferdinand Schoeman, „Gossip and privacy“, 1994.

390 Shaun B. Spencer, „The Surveillance Society and the Third-Party Privacy Problem“, *South Carolina Law Review* 65, 2 (2013): 375.

391 BDAR, 89 straipsnio 1 dalis.

392 Mireille Hildebrandt, „Location Data, Purpose Binding and Contextual Integrity: What's the Message?“, 2014, 31–62, https://doi.org/10.1007/978-3-319-05720-0_3; Franck Dumortier, „Facebook and Risks of „De-Contextualization" of Information“, Data Protection in a Profiled World, sud. Serge Gutwirth, Yves Poullet ir Paul De Hert (Dordrecht: Springer Netherlands, 2010): 119–137, https://doi.org/10.1007/978-90-481-8865-9_7.

393 Žr. disertacijos 1 skyrių.

nepaaiškinama, kaip ir kodėl jie iš viso turėtų būti renkami[394]. Duomenų rinkimo faktas, kalbant apie bepiločiu orlaivius, ir yra pats svarbiausias, todėl šiuo požiūriu kontekstinio integralumo teorija būtų sunkiai pritaikoma. Teisės aktai, kurie remtųsi H. Nissenbaum modeliu, nenagrinėtų, ar bepiločiu orlaiviu surinkti duomenys trečiojo asmens duomenų bazėje atsidūrė teisėtai, o veikiau koncentruotųsi į jau surinktos informacijos tolesnio perleidimo ir lyginimo tarpusavyje teisėtumą. Tad našta nustatyti, ar duomenys buvo surinkti teisėtai, tektų teismams arba tiesiog būtų nereguliuojama, t. y. duomenis bepiločiais orlaiviais būtų galima rinkti be apribojimų. Tiek vienu, tiek kitu atveju manytina, jog kontekstinio integralumo teorija nesuteiktų pakankamos privatumo apsaugos nuo pažeidimų, kuriuos gali sukelti nedideli bepiločiai orlaiviai.

3.2.2. Visuomeninės reikšmės filtro teorija

Apie privatumą viešojoje erdvėje rašė ir J. Reidenbergas. Jis siūlo teismams nustatant, ar buvo pažeistas asmens privatumas, taikyti savotišką „visuomeninės reikšmės filtrą“ vietoj JAV įtvirtinto „protingo privatumo lūkesčio“ (angl. *reasonable expectation of privacy*) testo. Jo siūlomo metodo esmė – atskirti viešai prieinamą informaciją, kuri turi visuomeninę reikšmę ir laikoma vieša, nuo viešai prieinamos informacijos, bet neturinčios visuomeninės reikšmės, – štai šią, J. Reidenbergo nuomone, ir reikėtų laikyti privačia[395]. Aiškindamas, kokia informacija jo teorijoje būtų laikoma privačia, o kokia visuomeninės reikšmės, J. Reidenbergas remiasi pavyzdžiais iš JAV teismų praktikos.

Pvz., aiškindamas tai, kas turėtų būti vadinama privačia informacija, kaip atspirties tašką J. Reidenbergas aptaria Katzo bylą, kurioje JAV Federalinių tyrimų biuro (toliau – FTB) agentai įtardami, kad fizinis asmuo (pavarde Katzas) vykdo nusikalstamą veiką, neturėdami teismo leidimo prie viešos telefono būdelės, kuria naudojosi įtariamasis Katzas, pritaisė pasiklausymo prietaisą. Pasinaudojant garso įrašu Katzas buvo nuteistas už tai, kad vykdė nusikalstamą veiką, bet vėliau JAV Aukščiausiojo Teismo buvo išteisintas, nes būdamas telefono būdelėje jis turėjo pagrįstą privatumo lūkestį, o FTB agentai neteisėtai klausėsi jo pokalbių be teismo leidimo[396]. J. Reidenbergas sutinka su šios bylos motyvacija ir antrina, jog naudojimasis telefonu viešoje telefono būdelėje vargu ar galėtų būti suvokiamas kaip „visuomenei reikšmingas“. Todėl, taikant J. Reidenbergo modelį, tokio pobūdžio veiksmai vertintini kaip privatūs, o bylos baigtis būtų tokia pati[397]. Kitoje byloje,

394 Pasak H. Nissenbaum, vieša stebėsena (angl. *public surveillance*), arba, kitaip tariant duomenų rinkimas, visiškai nepatenka į autorės siūlomo normatyvinio modelio taikymo sritį. Žr. Helen Nissenbaum, „Privacy as Contextual Integrity Symposium – Technology, Values, and the Justice System“, *Washington Law Review* 79, 1 (2004): 133–36.

395 Reidenberg, „Privacy in Public“, *supra note,* 50: 141–60.

396 „Katz v. United States“, No. 389 U.S. 347 (Supreme Court of the United States 1967 m. gruodžio 18 d.).

397 Reidenberg, „Privacy in Public“, *supra note,* 50: 155.

pobūdžio veiksmai vertintini kaip privatūs, o bylos baigtis būtų tokia pati. Kitoje byloje, vadinamoje „Whalen“, Niujorko valstija priėmė teisės aktą, kuriuo įvedė reikalavimą sukurti centralizuotą išduotų receptų valstybės kontroliuojamiems vaistams registravimo sistemą. JAV Aukščiausiasis Teismas pripažino, kad priimtas įstatymas neprieštarauja konstitucijai, nes duomenys apie asmenis, įrašytus į registrą, ir taip buvo atskleisti trečiosioms šalims – vaistinėms, todėl asmenys, įrašyti į registrą, negalėjo pagrįstai tikėtis privatumo pagal tradicinį „protingo privatumo lūkesčio“ standartą[398]. J. Reidenbergo nuomone, taikant jo siūlomą viešosios reikšmės filtrą, „Whalen“ bylos baigtis turėtų būti priešinga, nes gydytojų pacientams išrašomi receptai nėra reikšmingi visuomenei. Pasak autoriaus, recepto išdavimas yra veikiau privatus santykis tarp gydytojo, paciento ir vaistinės[399], o ne tarp paciento ir visuomenės.

J. Reidenbergo nuomone, ar konkrečiu atveju informacija bus suvokiama kaip visuomeninės reikšmės, turėtų būti vertinama ne pagal subjektyvius individo norus, o veikiau pagal socialines normas, kurios apibrėžia viešąjį interesą[400]. Kaip pavyzdį šiam teiginiui iliustruoti autorius aptaria „Reed“ bylą. Joje grupė Vašingtono valstijos piliečių pasirašė peticiją surengti referendumą, kurio tikslas būtų panaikinti valstijos įstatymą, išplečiantį tos pačios lyties partnerių pilietines teises[401]. Referendumas galiausiai buvo surengtas ir nedidele balsų persvara ginčijamas teisės aktas buvo paliktas galioti. Peticijos oponentai vadovaudamiesi teisės aktu, kuriuo leidžiama gauti viešų įrašų kopijas, kreipėsi į valdžios institucijas, kad šios pateiktų jiems peticijos kopiją. Peticijos šalininkai kreipėsi į teismą prašydami neleisti atskleisti pasirašiusių asmenų tapatybių. Byla galiausiai pasiekė JAV Aukščiausiąjį Teismą, kuris sprendė, ar teisės aktas, kuriuo remiantis peticijos oponentai kreipėsi į valdžios institucijas su prašymu suteikti peticijos sąrašų kopijas, neprieštarauja JAV konstitucijai. Teismas padarė išvadą, kad viešas referendumo peticijų atskleidimas yra svarbus rinkimų proceso vientisumui, nes apsaugo ne tik nuo sukčiavimo, bet ir nuo paprastų klaidų, tokių kaip besidubliuojantys parašai, ar asmenų, neturinčių teisės balsuoti, parašai, todėl jų negalima laikyti privačia informacija. Pasak J. Reidenbergo, visuomenė turi pagrįstą viešąjį interesą žinoti peticiją pasirašiusių asmenų vardus, nes šie tarsi dalyvauja priimant kolektyvinį valdymo aktą. Todėl tokia informacija, taikant autoriaus siūlomą metodiką, turėtų būti traktuojama kaip visuomeninės reikšmės ir negalėtų būti laikoma privačia. Kitaip tariant, bylą vertinant per autoriaus siūlomą visuomeninės reikšmės filtrą, „Reed“ bylos baigtis būtų tokia pati.

Vertinant visuomeninės reikšmės filtro teoriją, ar ji būtų pakankamas pagrindas reguliuojant privatumo apsaugą bepiločių orlaivių kontekste, disertacijos

398 „Whalen v. Roe“, No. 429 U.S. 589 (Supreme Court of the United States 1977 m. vasario 22 d.).
399 Reidenberg, „Privacy in Public“, *supra note,* 50: 156.
400 *Ibid.,* 156.
401 „Doe v. Reed“, 561 U.S. 186 (2010).

autorius mano, kad taikant praktiškai vargu ar tai būtų naudingas įrankis. Visų pirma, remiantis J. Reidenbergo teorija, neaišku, kaip įstatymų leidėjai turėtų formuluoti privatumo apsaugos teisinį reguliavimą, todėl visa ginčų sprendimo našta tektų teismams. Šiuo požiūriu ji nesiskiria nuo dvinarės privatumo teorijos, kuri siūlo kiekvieną situaciją vertinti ad hoc. Vis dėlto, kaip jau aptarta ankstesniame disertacijos skyriuje, daugelis autorių pripažįsta, jog dabartinė reguliavimo aplinka nepakankama ir reikalauja papildomų mokslinių tyrimų bei įstatymų leidėjų įsikišimo[402]. Antra, ši teorija kritikuojama, nes gali būti sunkumų atskiriant visuomenės dėmesio vertą informaciją nuo privačios[403]. Apskritai JAV Aukščiausiojo Teismo jurisprudencijoje surinktą informaciją vengiama skirstyti į didelės ir mažos vertės[404]. Trečia, taikant visuomeninės reikšmės teoriją teismai grąžinami prie senos diskusijos apie teisės į privatų gyvenimą ir saviraiškos teisės kolizijos[405], todėl jokios pridėtinės vertės ginčų, susijusių su bepiločiais orlaiviais ir privatumo apsauga, kontekste nesuteikia.

3.2.3. Ribų valdymo teorija

Trečioji dėmesio verta privatumo viešojoje erdvėje teorija sukurta M. E. Kaminski[406]. Autorės teigimu, žmonės naudoja įvairias strategijas ir mechanizmus, kad pasiektų optimalų privatumo lygį. Tokios strategijos arba mechanizmai gali būti verbalinis elgesys, paraverbalinis elgesys (pvz., balso tonas), neverbalinis elgesys (pvz., judesiai), asmeninė erdvė, teritorija (pvz., daiktų naudojimas tam tikroje vietovėje siekiant sukurti uždangą), įvairūs kultūriniai mechanizmai. Pasak M. E. Kaminski, riboms viešojoje erdvėje sukurti žmonės gali naudoti įvairius aplinkos daiktus, tokius kaip durys ir sienos. Pvz., asmuo, kuris nori atsiskirti nuo kitų žmonių, gali pasislėpti už sienos ar durų. Jei jis nori bendrauti tik su vienu žmogumi, bet ne su visais, esančiais toje patalpoje, gali su tuo žmogumi kalbėtis labai tyliai arba uždaroje patalpoje, tikėdamasis, kad kiti pokalbio negirdės arba negalės suprasti jo esmės. Tarp ribų valdymo mechanizmų gali būti ir bendravimo trukmė, pokalbio atvirumas, sakoma tikrovę atitinkanti informacija ar meluojama, naudojami neverbaliniai ženklai (pvz., akių kontaktas)[407] ir pan. Autorė pastebi, kad netgi kultūrose, kurios privatumui, žvelgiant per dichotominę teoriją, neteikia didelės reikšmės, gali būti taikomi kiti elgesio mechanizmai, kuriais žmonės naudojasi valdydami savo socialinį prieinamumą kitiems individams[408].

---

402 Žr. disertacijos 1 skyrių.
403 Kaminski, *supra note,* 51: 1130.
404 „United States v. Stevens", 559 U.S. 460 (2010)", *Justia Law,* žiūrėta 2022 m. lapkričio 7 d., https://supreme.justia.com/cases/federal/us/559/460/.
405 Žr. Mindaugas Lankauskas, „Balansavimas tarp teisės į privatumą ir saviraiškos laisvės Europos žmogaus teisių teismo jurisprudencijoje", *Teisės problemos* 2, 56 (2007): 103–131.
406 Kaminski, *supra note,* 51.
407 *Ibid.,* 1133.
408 *Ibid.,* 1134.

M. E. Kaminski teigia, kad ribų valdymas labai priklauso nuo konteksto, bet tai nereiškia, kad žmonės visuomet skiria daug laiko bandydami išsiaiškinti tam tikro poelgio ar pašnekesio kontekstą. Jie veikiau intuityviai ieško trumpesnių kelių, naudojasi žinomais elgesio modeliais, remiasi išankstiniais nusistatymais savo aplinkos atžvilgiu, mokslininkai tai vadina „atsiskleidimo žanrais" (angl. *genres of disclosure*)[409]. Pasak autorės, keičiantis technologijoms ir socialinėms praktikoms, kartu keičiasi ir atsiskleidimo žanrai. Pvz., anksčiau, kai Londono gatvės nebuvo stebimos vaizdo kameromis, žmonės elgėsi vienaip, o dabar, kai jie žino, kad gatvėse apstu CCTV kamerų, elgiasi kitaip, t. y. užuot veikę pagal senąjį viešo elgesio gatvėje žanrą, dabar žmonės elgiasi taip, lyg būtų stebimi kitų asmenų[410].

Pasak M. E. Kaminski, toks privatumo viešojoje erdvėje modelis veikia dvejopai. Pirma, jis leidžia asmenims geriau apskaičiuoti, kiek jie savo privataus gyvenimo pageidauja atskleisti atitinkamoje situacijoje (angl. *allowing an individual to calculate her desired degree of disclosure*). Pvz., asmuo prieš pradėdamas darbą gali norėti emociškai „pasikrauti" sušokdamas kokį nors juokingą šokį biurų pastato ketvirtame aukšte prie savo rašomojo stalo, kurį nuo kitų bendradarbių skiria sienos. Jei šį asmenį informuotume, jog nuo šiol už jo biuro langų skraidys vaizdą įrašinėjantys bepiločiai orlaiviai, jis gali norėti keisti savo elgesį suprasdamas, kaip pasikeitė jį supanti aplinka. Autorės nuomone, keičiantis technologinei ir socialinei aplinkai, įstatymų leidėjai, vadovaudamiesi ribų valdymo teorija, turėtų numatyti pareigą apie būsimus pasikeitimus informuoti stebimąjį ir gauti jo sutikimą, kad šis galėtų atitinkamai keisti savo elgesį. Pasak M. E. Kaminski, tokia pareiga jau įtvirtinta daugelyje šiuolaikinių teisės aktų[411].

Antra, jis užkerta kelią nepageidaujamiems žmonių elgesio pokyčiams (angl. *preventing undesirable behavioral changes*). Pasak M. E. Kaminski, įstatymų leidėjai gali norėti išsaugoti tam tikrus žmonių elgesio žanrus ne dėl to, kad jie išskirtinai vertingi (nors gali būti ir dėl šios priežasties), o dėl to, kad alternatyvus, pasikeitęs elgesys gali turėti reikšmingų neigiamų pasekmių. Pvz., įstatymų leidėjas gali nuspręsti, kad ankstesniame pavyzdyje minėtam asmeniui kasrytinis šokis yra labai svarbus ir atsisakyti tokio elgesio jis nepageidautų, nes galbūt tik pašokęs tampa produktyvesnis, galbūt tokia ekspresijos forma yra svarbi jo emocinei būsenai darbe arba tiesiog tai jo asmenybės dalis ir pan. Bet kuriuo atveju tokį elgesį visuomenėje įstatymų leidėjas gali norėti išsaugoti[412] ir atitinkamai priimti teisės aktus, kurie, pvz., draudžia arba riboja vykdyti bepiločių orlaivių skrydžius šalia pastatų.

Ribų valdymo teorija bepiločių orlaivių kontekste galėtų būti karkasas naujiems teisės aktams, suteikiantiems privatumo apsaugą, ir naujai teismų praktikai. Tikriausiai esminis aspektas, kuris daro šią teoriją patrauklią, yra

409 Leysia Palen ir Paul Dourish, „Unpacking *Privacy* for a Networked World", Proceedings of the SIGCHI conference on Human factors in computing systems (2003), 8.

410 Kaminski, *supra note,* 51: 1135.

411 *Ibid.,* 1136.

412 *Ibid.,* 1137.

koncentracija į elgesio šablonus, kuriuos siekiama visuomenėje išsaugoti, o ne į konkrečias technologijos savybes ar informacijos tipus, kurie neva iš prigimties galėtų kelti grėsmę asmens privatumui. Kitaip tariant, M. E. Kaminski teorijoje pagrindinis vaidmuo tenka elgesio modeliams, kuriuos norima išsaugoti arba šiek tiek apriboti dėl patogesnio gyvenimo, o visi apribojimai naujo amžiaus technologijoms, tarp jų ir bepiločiams orlaiviams, kyla būtent iš to saugotino (ar ribotino) elgesio modelio. Kaip ribų valdymo teorija veiktų praktikoje aiškiau matyti iš konkrečių pavyzdžių, pateikiamų tolesniame 4.6 poskyryje.

Kaip matyti iš pavyzdžių, M. E. Kaminski reguliavimo modelio svarbus aspektas yra tas, jog kiekvieno elgesio šablono išsaugojimas (ar užgožimas) būtų įtvirtintas privalomo pobūdžio įstatymų leidėjo (ar vietinės valdžios subjekto) priimtu teisės aktu. Tuomet teismų praktikoje nekiltų diskusijų dėl to, koks yra visuotinai priimtinas elgesio standartas. Dėl tokio požiūrio teismai galėtų pereiti nuo sudėtingo vertinimo, ar bepiločiais orlaiviais surinkta informacija turėtų būti laikoma privačia (kaip yra įprasta pagal dvinarę teoriją), prie paprastesnės analizės – ar teisės akto siūlomos priemonės leidžia asmenims modifikuoti savo elgesį ir ar apskritai teisės aktu turėtų būti ribojami tam tikro elgesio šablonai visuomenėje. Kitaip tariant, teismų dėmesys būtų nukreipiamas nuo vertinimo, ar tam tikra informacija yra iš prigimties jautri, prie analizės apie technologinių pokyčių poveikį asmens savarankiškumui ir elgesiui[413].

Svarbu ir tai, jog M. E. Kaminski teorija yra ganėtinai paprasta, ją lengvai suprastų didžioji visuomenės dalis. Kitaip tariant, tai naudingas teisinio reguliavimo pagrindas, nes skatina visuomenę įsitraukti į teisinę diskusiją dėl jiems reikšmingų elgesio modelių, kuriuos jie nori apsaugoti, bet nepradėti diskusijų, pvz., apie galimai privatumą ribojančias bepiločių orlaivių technologines savybes. Taikant šį modelį žmonėms spręsti esminius dalykus, o techninius paliktų įstatymų leidėjams, kurie turi daugiau galimybių išsiaiškinti, kokiomis techninėmis priemonėmis žmonių pageidaujamą interesą apsaugoti. Savo ruožtu visuomenei labiau įsitraukus į sprendimų priėmimą ir ribų valdymo apsaugą būtų skatinamas visuomenės individualus bei grupinis savarankiškumas, taip pat ir autonomiškumas, o tai turėtų padėti išvengti atšalimo efekto.

Dar galima teigti, jog teisės aktų kūrimas pasinaudojant elgesio modeliais sumažintų tikimybę riboti technologinę pažangą nepagrįstai, palyginti su įstatymais, kurie ribotų konkrečias bepiločių orlaivių technologines savybes ar renkamos informacijos pobūdį. Taip pat ir teisės normas, paremtas ribų valdymo teorija, būtų lengviau keisti motyvuojant elgesio standartų ar technologiniais pasikeitimais.

413 Kaminski, *supra note,* 51: 1138–1139.

3.2.4.Poskyrio išvados. Teorinis pagrindas ateityje reguliuoti privatumą viešoje vietoje bepiločių orlaivių kontekste

Analizuojant privatumo viešojoje erdvėje mokslinę literatūrą buvo identifikuoti trys pagrindiniai moksliniame diskurse vyraujantys reguliavimo modeliai: H. Nissenbaum *kontekstinis integralumas,* J. Reidenbergo *visuomeninės reikšmės teorija* ir M. E. Kaminski *ribų valdymo teorija.* Kiekvienas iš šių modelių buvo vertintas kaip potencialus teorinis pagrindas kurti pažangų bepiločių orlaivių privatumo reguliavimą ir teismų praktiką.

Atliktas tyrimas parodė, kad pagal H. Nissenbaum teoriją nagrinėjamas jau surinktos informacijos tolesnio perleidimo bei lyginimo tarpusavyje teisėtumas, tačiau pats duomenų rinkimo faktas nėra toks svarbus. Bet kadangi bepiločiai orlaiviai yra informacijos rinkimo įrankis, tai ir duomenų rinkimo momentas yra pats svarbiausias, o remiantis kontekstinio integralumo teorija našta nustatyti, ar konkrečiu atveju duomenys buvo surinkti teisėtai, tektų teismams arba tai liktų nereguliuojama sritis, t. y. duomenis bet kokiose situacijose būtų galima rinkti be apribojimų. Tiek vienu, tiek kitu atveju kontekstinio integralumo teorija nesuteiktų pakankamos privatumo apsaugos nuo pažeidimų, kuriuos gali sukelti nedidelių bepiločių orlaivių naudojimas.

Vertinant J. Reidenbergo teoriją galima daryti išvadą, jog ji mažai skiriasi nuo dvinarės privatumo teorijos, kurią dauguma mokslininkų pripažįsta kaip nepakankamą naudoti bepiločių orlaivių kontekste. Taikant šią teoriją itin išaugtų krūvis teismams, kurie turėtų aiškintis, kuri teisė konkrečiu atveju viršesnė – teisė į privatumą ar teisė į saviraišką. Taigi, disertacijos darbo autoriaus nuomone, J. Reidenbergo visuomeninės reikšmės reguliavimo modelis jokios pridėtinės vertės sprendžiant ginčus, kylančius dėl bepiločių orlaivių ir privatumo apsaugos, neturi.

M. E. Kaminski savo teorijoje teisės aktų leidėjams ir teismams siūlo į privatumą viešojoje erdvėje žvelgti per ribų valdymą, dėmesį sutelkiant į elgesio modelius, kuriuos norma išsaugoti (arba neišsaugoti dėl didesnio gėrio). Pagrindinis dalykas, darantis šį reguliavimo modelį patrauklų, yra jo paprastumas, kuris ne tik sumažintų teismų darbo krūvį, bet ir leistų į diskusiją dėl to, kaip reguliuoti privatumą viešojoje erdvė, įsitraukti visuomenei. Kuo aktyviau visuomenė įsitrauks į sprendimų priėmimą ir ribų valdymo apsaugą, tuo labiau bus skatinamas individualus ir grupinis savarankiškumas bei autonomiškumas, o tai padės išvengti atšalimo efekto. Taip pat taikant šią teoriją būtų paprasčiau spręsti teisminius ginčus, kylančius dėl privatumo viešojoje erdvėje, kas ilgainiui užtikrintų, jog technologinė pažanga nebus nepagrįstai apribota.

M. E. Kaminski modeliu galėtų būti remiamasi kuriant naujus Lietuvos ir ES teisės aktus ar teismų praktiką, susijusią su privatumu viešojoje erdvėje, todėl tolesnėje disertacijoje dalyje ribų valdymo teorija naudojama kaip metodologinis pagrindas, kuriuo remiantis vertinama, ar teismų praktikoje ir teisės normose suformuluotos taisyklės ją atitinka.

3.3. Bepiločių orlaivių naudojimo viešojoje erdvėje ir privatumo santykis EŽTT ir Lietuvos jurisprudencijoje

3.3.1. Privatumo ir viešosios erdvės santykis EŽTT jurisprudencijoje

ES lygmeniu teisę į privatų gyvenimą įtvirtina EŽTK 8 straipsnis, numatantis pagarbą kiekvieno asmens privatumui ir šeimos gyvenimui, būsto neliečiamybei ir susirašinėjimo slaptumui. EŽTK 8 straipsnio 2 dalis papildomai numato, kad apriboti teisę į privatumą galima tik įstatymų nustatytais atvejais ir tada, kai demokratinėje visuomenėje tai būtina dėl valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesų, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai, moralei arba kitų asmenų teisėms ir laisvėms apsaugoti[414]. Kaip jau minėta, EŽTT yra nurodęs, kad šios teisės turinys toks platus, jog neįmanoma būtų prieiti prie baigtinio apibrėžimo[415], tačiau diskusijoje apie stebėseną bepiločiais orlaiviais nebūtina atskleisti visą teisės į privatumą turinį, svarbiausia būtų apibrėžti, kokios pagal EŽTT jurisprudenciją yra asmens privatumo ribos viešoje vietoje.

Pabrėžtina, kad nors EŽTK 8 straipsnio tikslas – apsaugoti asmenis nuo savavališko valdžios institucijų kišimosi į privatų gyvenimą, juo remiantis atsirastų ne tik negatyvi valstybės institucijų pareiga susilaikyti nuo kišimosi, bet ir pozityvi – gerbti asmenų teisę į privatų ir šeimos gyvenimą. Ši pozityvi pareiga galioja ir santykiams tarp privačių asmenų, jie taip pat turi gerbti vienas kito privatumą[416].

EŽTT požiūris į privatumą viešumoje paremtas „protingo lūkesčio standartu“, t. y. individas būdamas viešoje vietoje gali tikėtis privatumo, tačiau vertinant, ar tam tikru atveju teisė į privatumą buvo pažeista, reikia atsižvelgti į tokias aplinkybes kaip, pvz., ar stebėta sistemiškai ir ar padaryti įrašai buvo paskelbti viešai[417]. Taip pat pažymėtina, kad netgi sistemiškas stebėjimas vaizdo kameromis viešoje vietoje savaime nebūtų traktuojamas kaip privatumo pažeidimas. Pvz., byloje apie asmenų stebėjimą viešose vietose, kai duomenys nėra įrašomi, teismas yra pasisakęs, jog tokia stebėsena savaime nebūtų laikoma privatumo pažeidimu[418].

Vertinant tuos atvejus, kai buvo taikytas EŽTK 8 straipsnis, svarbu nustatyti, ar individas buvo stebimas tikslingai[419] ir ar surinkti asmens duomenys

---

414 EŽTK

415 Žr. disertacijos 1.3. poskyrį; „Costello-Roberts v. The United Kingdom“, 89/1991/341/414, Council of Europe: European Court of Human Rights, 23 February 1993.

416 „Söderman v. Sweden”, No. 5786/08 (ECtHR [GC] 2013 m. lapkričio 12 d.); „Von Hannover v. Germany (no. 2)”, No. 40660/08, 60641/08 (ECtHR [GC] 2012 m. vasario 7 d.).

417 „P. G. and J. H. V. the United Kingdom”, No. 44787/98 (ECtHR 2001 m. rugsėjo 25 d.); „Bărbulescu v. Romania”, No. 61496/08 (ECtHR [GC] 2017 m. rugsėjo 5 d.); „Antović and Mirković v. Montenegro“, No. 70838/13 (ECtHR 2017 m. lapkričio 28 d.).

418 „Herbecq and the Association „Ligue Des Droits De L'homme“ v. Belgium (dec.)”, No. 32200/96, 32201/96 (EComHR 1998 m. sausio 14 d.).

419 „Perry v. the United Kingdom”, No. 63737/00 (ECtHR 2003 m. liepos 17 d.); „Köpke v. Germany (dec.)”, No. 420/07 (ECtHR 2010 m. spalio 5 d.); „Vukota-Bojic v. Switzerland”, No. 61838/10 (ECtHR 2016 m. spalio 18 d.).

buvo apdoroti, panaudoti ar paviešinti tokiu būdu, kuris stebėtam asmeniui buvo netikėtas[420]. Teismas yra pasisakęs, kad net viešose vietose sistemingas arba nuolatinis identifikuotų asmenų vaizdo įrašymas ir vėlesnis tos užfiksuotos medžiagos apdorojimas gali kelti klausimų dėl asmenų privatumo pažeidimo[421].

Darbo vieta taip pat gali būti traktuojama kaip vieša, todėl aktuali ir jurisprudencija dėl darbo vietos stebėjimo. Vienoje tokių bylų EŽTT pripažino, kad net ir darbo vieta ne visada laikoma vieša, nurodydamas, jog EŽTK 8 straipsnyje „būsto" terminas gali būti aiškinamas kaip įtraukiantis profesinę veiklą ar patalpas, ypač kalbant apie asmenį, kuris verčiasi laisvąja profesija (byloje pareiškėjas buvo teisininkas)[422].

Kitoje byloje darbdavys darbo vietoje, darbuotojui nežinant, buvo įrengęs vaizdo stebėjimo kameras, kuriomis galėjo stebėti darbuotoją ir duomenis įrašinėti apie penkiasdešimt valandų per dviejų savaičių laikotarpį. Įrašus darbdavys pateikė darbo ginčus nagrinėjusiems teismams, kad įrodytų, jog darbuotoją iš darbo atleido teisėtai. EŽTT šiuo atveju nusprendė, kad buvo pažeista darbuotojo teisė į privatų gyvenimą[423]. Neslaptą universiteto lektorių paskaitų vaizdo įrašinėjimą (be garso), siekiant ne tik užtikrinti saugumą auditorijose, bet ir stebėti mokymo procesą, kai šie įrašai buvo saugomi apie mėnesį, o juos peržiūrėti galėjo tik fakulteto dekanas, – teisėjų kolegija vos vieno balso persvara (keturi prieš tris) pripažino, kaip pažeidžiantį pareiškėjų teisę į privatų gyvenimą[424]. Pagrindinis EŽTT argumentas šiuo atveju buvo tai, jog pagal nacionalinę teisę asmens duomenis be sutikimo buvo galima rinkti tik siekiant užtikrinti saugumą, o ne mokymo procesui stebėti[425]. Auditorija laikytina vieša ar privačia, teismas *expressis verbis* nepasisakė, bet nurodė, jog tai erdvė, kurioje dėstytojai ne tik moko, bet ir bendrauja su studentais, čia konstruojamas socialinis identitetas[426]. Pasak dviejų atskirąją nuomonę išdėsčiusių teisėjų, teismas galėjo pasisakyti plačiau, t. y. vertindamas atsižvelgti ne tik į nacionalinės teisės aktuose numatytus duomenų rinkimo tikslus, bet ir į protingą lūkestį. Jų nuomone, universiteto auditorijos negalima laikyti nei vieša, nei privačia vieta. Joje tarp dėstytojo ir studentų per semestrą ar metus užsimezga tam tikri santykiai, dėl to auditorijoje dėstytojas gali elgtis taip, kaip galbūt niekada nesielgtų už jos ribų. Kitaip tariant, dėstytojas auditorijoje turi apsaugą nuo „nepageidaujamo dėmesio". Tačiau, pasak atskirąją nuomonę išdėsčiusių teisėjų, tai nereiškia, kad paskaita iš viso negalėtų būti įrašinėjama. Išimtys turėtų būti taikomos, pvz., tais atvejais, kai auditorijoje paskaitos klausantys studentai ją įrašinėja mokymo tikslais arba kai įrašu planuoja naudotis studentai, negalėję dalyvauti paskaitose[427].

---

420 „Perry v. the United Kingdom"; „Vukota-Bojic v. Switzerland".
421 „López Ribalda and Others v. Spain", *supra note,* 142.
422 „Niemietz v. Germany", No. 13710/88 (ECtHR 1992 m. gruodžio 16 d.).
423 „Köpke v. Germany (dec.)", *supra note,* 418.
424 „Antović and Mirković v. Montenegro", *supra note,* 421.
425 *Ibid.,* 59.
426 *Ibid.,* 44.
427 *Ibid.,* Joint concurring opinion of judges Vučinić and Lemmens.

Atskirąją nuomonę išdėstė ir kiti trys teisėjai byloje. Jų nuomone, šiuo atveju pareiškėjų teisė į privatų gyvenimą nebuvo pažeista. Universiteto auditorija, teisėjų nuomone, yra kvazivieša vieta, kurioje dėstytojai negali tikėtis tokios privatumo apsaugos kaip ir savo kabinetuose[428].

Detaliau reikėtų aptarti „López Ribalda and Others v. Spain" bylą[429] apie darbuotojų privatumą darbo vietoje, kurioje teismas nustatė ypač daug universalaus taikymo teisės taisyklių. Šiuo atveju darbdavys įrengė slaptas vaizdo kameras darbo vietoje įtardamas, kad darbuotojai vagia iš parduotuvės, kurioje dirba. Teismas, išnagrinėjęs bylą, pripažino, kad pareiškėjų teisė į privatų gyvenimą buvo apribota pagrįstai[430].

Teisėjų kolegija bylos motyvacinėje dalyje nustatė kriterijus, pagal kuriuos nacionaliniai teismai turėtų vertinti, ar vaizdo stebėjimo priemonės darbo vietoje buvo proporcingos:

1. Ar darbuotojui buvo pranešta apie planuojamas įdiegti vaizdo stebėjimo priemones ir jų įgyvendinimą? Nors darbuotojai gali būti informuojami įvairiais būdais, tačiau, atsižvelgiant į konkrečias aplinkybes, pranešime turėtų būti aiškiai nurodytas stebėjimo pobūdis. Taip pat svarbu, kad informacija būtų pateikta prieš įdiegiant stebėjimo priemones.

2. Darbdavio stebėjimo mastas ir įsibrovimo į darbuotojo privatumą laipsnis – reikėtų atsižvelgti į privatumo lygį stebimoje srityje, taip pat į visus laiko ir erdvės apribojimus bei žmonių, turinčių prieigą prie stebėjimo rezultatų, skaičių.

3. Ar darbdavys nurodė priežastis, pateisinančias stebėjimą, jo mastą? Kuo įkyresnis stebėjimas, tuo svarbiau jį pagrįsti.

4. Ar buvo galima stebėsenos sistema, kuri taikytų mažiau įkyrius metodus ir priemones darbuotojams stebėti? Tik atsižvelgiant į konkrečias aplinkybes reikėtų įvertinti, ar darbdavio tikslas galėjo būti pasiektas mažiau kišantis į darbuotojo privatumą.

5. Kokios stebėsenos pasekmės darbuotojui, kuriam ji taikyta? Pirmiausia reikėtų atsižvelgti į tai, kaip darbdavys pasinaudojo stebėsenos rezultatais ir ar tie rezultatai padėjo siekti numatyto tikslo.

6. Ar darbuotojui buvo suteiktos tinkamos apsaugos priemonės, ypač tada, kai darbdavio vykdomas stebėjimas įkyraus pobūdžio? Tarp tokių apsaugos priemonių gali būti darbuotojų arba darbuotojų atstovų informavimas apie įrengtą stebėjimą bei jo mastą, taip pat nepriklausomų institucijų informavimas arba galimybė pateikti skundą[431].

Pasak teisėjų kolegijos, vertinant stebėsenos proporcingumą būtina atsižvelgti į vietas, kuriose buvo stebima ir kokios privatumo apsaugos ten pagrįstai galėjo tikėtis darbuotojas. Asmens privatumo lūkesčiai labai dideli vietose, kurios

428 *Ibid.,* Joint concurring opinion of judges Spano, Bianku and Kjølbro.
429 „López Ribalda and Others v. Spain", *supra note,* 146.
430 *Ibid.,* 137.
431 *Ibid.,* 116.

iš prigimties yra privačios, pvz., tualetuose ar rūbinėse, kur pateisinama sustiprinta apsauga ar net visiškas vaizdo stebėjimo draudimas. Privatumo lūkesčiai yra aukšti ir uždarose darbo vietose, tokiose kaip darbo kabinetai. Tačiau jie akivaizdžiai mažesni tose vietose, kurios yra matomos ar prieinamos kolegoms arba plačiai visuomenei[432].

Išnagrinėjus bylą buvo išdėstyta ir trijų teisėjų atskiroji nuomonė, jog naujos technologijos dramatiškai pagerino vaizdo stebėjimo ir perdavimo galimybes, todėl teismas galėjo apie stebėseną pasisakyti plačiau. Vis dėlto teisėjų kolegijos dauguma pasirinko pateikti sprendimą tik atsižvelgiant į bylos faktines aplinkybes, o dėl privatumo apsaugos kituose kontekstuose nesiplėsti[433].

Dar vienas ypač svarbus EŽTT sprendimas, kurį bepiločių orlaivių kontekste vertėtų aptarti atskirai, yra „Big Brother Watch and Others v. the United Kingdom"[434]. Pasak byloje atskirąją nuomonę išdėsčiusių teisėjų, „retai pasitaiko atvejų, kai teismui tenka spręsti bylą, kuri formuos visuomenės ateitį. Dabartinis pavyzdys yra toks."[435] Net aštuonerius metus trukusį ginčą po 2013 m. Edwardo Snowdeno skandalo[436], per kurį buvo atskleistos JAV ir JK masinės stebėsenos programos, iškėlė pareiškėjų grupė sudaryta iš šešiolikos asmenų. Pareiškėjai iš esmės teigė, kad slapto sekimo programas JK vykdė neteisėtai. Disertacijos problematikos kontekste svarbiausia yra teismo motyvacija dėl valstybių masinės slaptos stebėsenos režimų teisėtumo pagal EŽTK 8 straipsnį.

Bylą pirmiausia nagrinėjo žemieji EŽTT rūmai, kurių nuomone, JK stebėsenos programa pažeidė EŽTK 8 straipsnį[437], tačiau teismas pripažino, kad valstybių nacionalinės valdžios institucijoms suteikiama gana plati diskrecija sprendžiant, kokių priemonių reikėtų imtis siekiant užtikrinti nacionalinį saugumą[438], ir masinės slaptos stebėsenos režimai *per se* šių ribų neperžengė[439]. Aukštieji EŽTT rūmai su šia motyvacija iš esmės sutiko pabrėždami, kad masinė stebėsena susitariančioms valstybėms yra gyvybiškai svarbi siekiant identifikuoti grėsmes nacionaliniam saugumui[440].

Tačiau šios bylos atveju teismas nusprendė, kad JK masinės komunikacijų stebėsenos režimas pažeidžia EŽTK 8 straipsnį dėl trūkumų, kurie lėmė, jog režimo taikytas per plačiai ir netenkino „teisės kokybės" reikalavimo, tad negalėjo išlaikyti tokio įsiveržimo į asmens privatumą lygio, kuris „būtinas demokratinėje

---

432 „López Ribalda and Others v. Spain", *supra note,* 146: 125.
433 Ibid., Joint dissenting opinion of judges De Gaetano, Yudkivska and Grozev 4.
434 „Big Brother Watch and Others v. the United Kingdom", No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 2021 m. gegužės 25 d.).
435 *Ibid.,* Joint partly dissenting opinion of judges Lemmens, Ranzoni and Bošnjak 1.
436 „How the US Spy Scandal Unravelled", *supra note,* 182.
437 „Big Brother Watch and Others v. the United Kingdom", *op. cit.* (ECtHR 2018 m. rugsėjo 13 d.).
438 *Ibid.,* 308.
439 *Ibid.,* 314.
440 „Big Brother Watch and Others v. the United Kingdom", *supra note,* 438: 424.

visuomenėje“[441]. Teismas nustatė, kad JK ryšių duomenų įgijimas iš ryšių paslaugų teikėjų (vadinama „II skyriaus režimu“) taip pat pažeidė 8 straipsnį, nes neapribojo prieigos prie duomenų tik kovos su „sunkiais nusikaltimais“ tikslais ir nereikalavo išankstinės teismo ar kitos nepriklausomos administracinės priežiūros institucijos peržiūros[442].

Galiausiai teisėjų kolegijos dauguma (dvylika iš septyniolikos) nusprendė, kad dalijantis informacija, nors JK valdžios institucijos gavo stebėsenos medžiagą iš užsienio žvalgybos tarnybų, bet EŽTK 8 straipsnio nepažeidė[443]. Pasak teismo, dalijimasis žvalgybos duomenimis yra leistinas esant tam tikroms apsaugos priemonėms: (1) nacionalinėje teisėje turi būti aiškiai nurodytos aplinkybės, kuriomis toks perdavimas gali įvykti; (2) perduodančioji valstybė turi gauti iš priimančiosios valstybės garantijas dėl tinkamo informacijos saugojimo ir apriboti tolesnį jos atskleidimą. Tačiau, kaip teismas kitoje byloje išaiškino šias sąlygas, tai nebūtinai reiškia, kad priimančioji valstybė turi turėti panašią apsaugą į perduodančiąją valstybę; taip pat nebūtinai reiškia, kad minėtos garantijos būtų pateiktos prieš kiekvieną perdavimą[444].

Penki teisėjai šioje byloje išdėstė atskirąsias nuomones, iš kurių trys nurodė, kad teismo sprendimas nesuteikia jokios aiškios materialios apsaugos prieš neproporcingą stebėsenos režimų kišimąsi į asmenų privatų gyvenimą[445] ir kad masinei stebėsenai turėtų būti reikalingas teismo leidimas[446]. Pinto de Albuquerque, vieno iš teisėjų, nuomone, masinės stebėsenos programos visiškai prasilenkia su proporcingumo principu, o pagal teismo sprendimą valstybėms suteikiamos tokios plačios diskrecijos ribos, jog net griežčiausia jų priežiūra mažai apsaugotų asmenis nuo valstybės institucijų piktnaudžiavimo[447].

Moksliniame diskurse šis EŽTT sprendimas taip pat sulaukė kritikos. Pvz., pasak M. Žalnieriūtės, EŽTT laikosi procedūralistinės metodikos, kuria vadovaujantis dėmesys sutelkiamas ne į materialinį masinių stebėsenos režimų teisėtumą ar faktinį jų veiksmingumą, o vien į procedūrines priemones, kurios neva turėtų apsaugoti privatumą[448]. M. Žalnieriūtė turi omeny 8 procedūrinius masinių stebėsenos režimų kriterijus, kuriuos valstybės turėtų perkelti į savo nacionalinius teisės aktus, t. y. valstybių nacionaliniai teisės aktai turėtų numatyti:

1. Pagrindus, kuriais remiantis gali būti leista vykdyti masinę stebėseną.
2. Aplinkybes, kuriomis asmens susižinojimas gali būti stebimas.

---

441 *Ibid.,* 426.
442 *Ibid.,* 524–525.
443 *Ibid.,* 514, 516.
444 „Centrum För Rättvisa v. Sweden“, No. 35252/08 (ECtHR [GC] 2021 m. gegužės 25 d.).
445 „Big Brother Watch and Others v. the United Kingdom“, *supra note,* 438: Joint partly dissenting opinion of judges Lemmens, Ranzoni and Bošnjak 14.
446 *Ibid.,* Joint partly dissenting opinion of judges Lemmens, Ranzoni and Bošnjak, 23–24.
447 *Ibid.,* Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque.
448 Monika Zalnieriute, „Procedural Fetishism and Mass Surveillance under the ECHR“, *Verfassungsblog: On Matters Constitutional* (2021), 6.

3. Leidimų vykdyti stebėseną išdavimo tvarką.

4. Procedūras, kurių privaloma laikytis renkant, tiriant ir naudojant stebėsenos metu surinktą medžiagą.

5. Atsargumo priemones, kurių reikia imtis perduodant medžiagą kitoms šalims.

6. Stebėsenos trukmės apribojimus, sąlygas surinktos informacijos saugojimui ir aplinkybes, kuriomis surinkta informacija turi būti ištrinta ir sunaikinta.

7. Nepriklausomos priežiūros institucijos veikimo procedūras ir sąlygas, kuriomis vadovaujantis priežiūros institucija galėtų užtikrinti aukščiau nurodytų kriterijų laikymąsi, jos galias atvejais, kai kriterijų nesilaikoma.

8. Nepriklausomos priežiūros institucijos veikimo procedūras ir sąlygas, pagal kurias ši institucija galėtų vykdyti *ex post facto* atitikties peržiūrą, jos galias atvejais, kai kriterijų nesilaikoma[449].

Pasak atskirąją nuomonę išdėsčiusio teisėjo P. de Albuquerque, teismas šiuos kriterijus išreiškė „nepriimtinai miglotomis" sąvokomis[450]. Taigi reikėtų suprasti, jog vieno ar kelių kriterijų nesilaikymas tikriausiai nelemtų neatitikties[451]. Negana to, kaip teigia teisėjas, bendras konsensusas Europoje yra atsisakyti masinės stebėsenos, nes ši nėra veiksminga priemonė terorizmo prevencijai[452], tačiau šį požiūrį teismas pasirinko ignoruoti[453].

Bendrą atskirąją nuomonę išdėstę teisėjai Lemmensas, Vehabovićius ir Bošnjakas teigia, jog naujųjų kriterijų nereikėtų laikyti minimaliais standartais, kuriais remiantis būtų užtikrinta privatumo apsauga, priešingai, jie individams nesuteikia jokios aiškios materialinės apsaugos nuo neproporcingo valstybės kišimosi į jų teises[454].

ESTT, kuris anksčiau buvo tarsi privatumo vėliavnešys dėl daugelio sprendimų, palankių asmens teisei į privatų gyvenimą, kaip pastebi M. Žalnieriūtė, po šio rezonansinio EŽTT sprendimo, deja, jau laikosi panašios, privatumui nepalankios, motyvacijos kaip ir EŽTT[455], o tai veda prie labai pavojingo konsensuso

---

449 „Big Brother Watch and Others v. the United Kingdom", *supra note,* 438: 335; „Weber and Saravia v. Germany (dec.)", No. 54934/00 (ECtHR 2006 m. birželio 29 d.).

450 „Big Brother Watch and Others v. the United Kingdom", *supra note,* 438: Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque, 2.

451 Monika Zalnieriute, „Big Brother Watch and Others v. the United Kingdom", *American Journal of International Law* 116, 3 (2022): 585–592, https://doi.org/10.1017/ajil.2022.35.

452 Council of Europe Human Rights Commissioner's Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, CommDH (2016)20, 2016; Council of Europe Parliamentary Assembly resolution on Terrorist attacks in Paris: together for a democratic response, 2015.

453 „Big Brother Watch and Others v. the United Kingdom", *supra note,* 438: Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque, 8.

454 *Ibid.,* Joint partly dissenting opinion of judges Lemmens, Ranzoni and Bošnjak.

455 Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others, ECLI:EU:C:2020:791, Grand Chamber Judgment, at 136 (Ct. Just. Eur. Union Oct. 6, 2020), at http://curia.europa.eu/juris/document/ document.jsf?text¼&docid¼232084&pageIndex¼0&doclang¼EN&mode¼lst&dir¼&occ¼first&part¼ 1&cid¼6166350.

tarptautinėje justicijoje, kai palaikomas masinės stebėsenos režimų prima facie teisėtumas[456]. Be jokios abejonės, „Big Brother Watch" sprendimas turės didelę įtaką stebėsenos teisiniam reguliavimui ateityje. Teisėjas P. de Albuquerque įspėja, jog „teismo atsainus požiūris į teisinių standartų formavimą gali pasirodyti labai patrauklus kai kuriuose Europos kampeliuose uoliai dirbančioms slaptosioms tarnyboms, dėl to anksčiau ar vėliau kentės ne kas kitas, o nekalti žmonės"[457].

3.3.2. Privatumo ir viešosios erdvės santykis Lietuvos jurisprudencijoje

Vykdant skrydžius bepiločiu orlaiviu viešoje vietoje sutikimą gauti gali būti ypač sudėtinga[458], todėl vadovautis šiuo privatumo ribojimo pagrindu Lietuvos teisėje tokius skrydžius vykdantiems privatiems subjektams, disertacijos autoriaus vertinimu, labiausiai tikėtina.

Lietuvos teisės aktuose privatumo ribojimas, kai duomenys renkami viešoje vietoje, yra įtvirtintas teisės į atvaizdą reglamentavime. CK 2.22 straipsnis numato, jog asmens atvaizdas gali būti atgaminamas, parduodamas, demonstruojamas, spausdinamas ir fotografuojamas be individo sutikimo, *inter alia,* jeigu fotografuojama viešoje vietoje[459]. Kadangi CK 2.22 straipsnis tiesiogiai būtų taikomas tik vaizdo įrašymo atveju, kiek painiau yra su garso ar kitokių asmens duomenų įrašymu. Nuo neteisėto pasiklausymo ir kitokio stebėjimo apsaugą suteikia CK 2.23 straipsnis. Jame nurodoma, kad „privataus gyvenimo pažeidimu", *inter alia,* būtų laikomas neteisėtas asmens stebėjimas, asmens telefoninių pokalbių, susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų ir informacijos konfidencialumo pažeidimas[460]. Tačiau, kas konkrečiai būtų laikoma neteisėtu stebėjimu, korespondencijos ar informacijos konfidencialumo pažeidimu, įstatymas nedetalizuoja. Panaši nuostata įtvirtinta ir LR visuomenės informavimo įstatyme (toliau – Visuomenės informavimo įstatymas), tačiau jame teisės normos formuluotė suteikia erdvės aiškesnei interpretacijai. Visuomenės informacijos įstatymas „draudžia" be sutikimo daryti garso ar vaizdo įrašus asmens gyvenamojoje patalpoje, privačioje namų valdoje ir jai priklausančioje aptvertoje ar kitaip aiškiai pažymėtoje teritorijoje, nepaisant to, ar tas asmuo yra nurodytose vietose[461]. Draudimo Visuomenės informacijos įstatymas *expressis verbis* nenumato informaciją renkant viešose vietos. Todėl galimas aiškinimas, jog informacijos rinkimas viešoje vietoje yra ne tik teisės į atvaizdą, bet ir vienas iš platesnės teisės į privatų gyvenimą ribojimo pagrindų.

---

456 Zalnieriute, „Big Brother Watch and Others v. the United Kingdom", *supra note,* 452: 591.
457 Big Brother Watch and Others v. the United Kingdom, *supra note,* 438: Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque 15.
458 Žr. disertacijos 2.3.2 poskyrį; disertacijos 4.2.1 poskyrį.
459 Civilinis kodeksas, 2.22 straipsnis.
460 *Ibid.*
461 Visuomenės informavimo įstatymas, 13 straipsnio 1 dalies 1 punktas.

Tokį aiškinimą pastiprina ir tai, jog Lietuvos teismų praktikoje teisė į atvaizdą ir teisė į privatų gyvenimą dažnai ginamos kartu[462]. EŽTT bylose garso įrašymo ir atvaizdo įrašymo nediferencijuoja – teismas vertinimą atlieka tiesiog abstrakčiai per teisę į privatumą, o ne per teisę į atvaizdą ir teisę į privatumą atskirai. EŽTK ir Lietuvos teisinėje sistemoje teisės į privatų gyvenimą reglamentavimo būdas šiek tiek skiriasi, nors iš esmės į privatumo sąvoką pagal abi sistemas įeina tie patys elementai. Kaip minėta, privataus gyvenimo apsaugą EŽTK garantuoja 8 straipsnis, kuriame nėra *expressis verbis* įvardyta teisė į atvaizdą, bet tai, jog ji įeina į EŽTK 8 straipsnio turinį, patvirtina EŽTT[463]. Lietuvoje teisė į atvaizdą (CK 2.22 straipsnis) ir teisės į privatų gyvenimą (CK 2.23 straipsnis) įtvirtintos atskiruose straipsniuose. Taigi didelio skirtumo nuo EŽTT praktikos Lietuvos teisinėje sistemoje šiuo aspektu nėra. Disertacijos autoriaus vertinimu, pagal Lietuvos teisę viešos vietos išimtis turėtų būti taikoma bepiločiais orlaiviais įrašant ne tik vaizdą, bet ir garsą bei kitą asmens duomenis galinčią atskleisti informaciją. Tiesa, didžiojoje jurisprudencijos dalyje LAT aiškinimą atlieka vien per teisę į atvaizdą. Tačiau, vadovaujantis EŽTT praktika, tokį aiškinimą reikėtų suprasti kaip *mutatis mutandis* taikytiną ir teisės į privatų gyvenimą apsaugai, įskaitant ir apsaugą nuo neteisėtos viešoje vietoje bepiločių orlaivių jutikliais vykdomos (vaizdo, garso, šilumos pėdsakų, duomenų ryšio ir pan.) stebėsenos.

Svarbu paminėti, jog net ir esant ribojimo pagrindams, tarp jų ir fiksuojant asmens duomenis viešoje vietoje, Lietuvoje, kaip ir kitose kontinentinės tradicijos šalyse, laikomasi garbės ir orumo apsaugos. Pagal CK 2.22 straipsnio 3 dalį nuotraukų (jų dalies), netgi jeigu jos užfiksuotos teisėtai, nebūtų galima demonstruoti, atgaminti ar parduoti, jeigu tai pažemintų asmens garbę, orumą ar dalykinę reputaciją[464]. Pagal CK 2.24 straipsnį tokia pati apsauga būtų suteikiama ir garso įrašymo atveju.

Pereinant konkrečiai prie privatumo ribų viešoje vietoje, Kasacinio teismo praktikoje aiškinama, kad asmuo, net ir būdamas viešoje vietoje, nepraranda savo individualumo ir privatumo. Kilus klausimui dėl teisės į atvaizdą ribojančios normos taikymo, būtina atsižvelgti į konkrečioje byloje nustatytas reikšmingas aplinkybes ir netaikyti nurodytos teisės normos formaliai, pvz., tik konstatavus, kad fotografuota ne privačioje teritorijoje[465].

Tai, kas apibendrintai būtų laikoma „vieša vieta“, nei Lietuvos teismų praktikoje, nei teisės aktuose nerasime, tačiau, pasak CK komentaro autorių, tai gali būti gatvė, parduotuvė, parkas, teatras, valstybės įstaiga, restoranas, bankas[466]. Lietuvos įstatymuose šio termino apibrėžimą galima

462 Žr. LAT Civilinių bylų skyriaus 2008 m. rugsėjo 23 d. nutartis civilinėje byloje Nr. 3K-3-394/2008.

463 „Peck v. the United Kingdom“, No. 44647/98 (ECtHR 2003 m. sausio 28 d.).

464 Civilinis kodeksas, 2.22 straipsnio 3 dalis.

465 LAT 2008 m. rugsėjo 23 d. nutartį civilinėje byloje Nr. 3K-3-394/2008.

466 Valentinas Mikelėnas ir kt., *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys* (Vilnius: Justitia, 2002), 57.

rasti fragmentiškai. Pvz., LR triukšmo valdymo įstatymas prie viešų vietų priskiria miestų, gyvenviečių gatves, aikštes, parkus, skverus, bendro naudojimo pastatus, barus, diskotekas, kavines, pramoginius renginius[467]. LR susirinkimų įstatymas nurodo, jog susirinkimai gali būti vykdomi tokiose viešose vietose kaip gyvenamųjų vietovių gatvės, aikštės, parkai, skverai ir bendrojo naudojimo pastatai[468]. Lietuvos teismų praktikoje apie tai, kas patektų į viešosios erdvės ribas, galima nebent spręsti iš konkrečiose bylose nagrinėjamų situacijų. Pvz., vieša vieta būtų laikomos kapinės[469], parduotuvės prekybos salė[470].

Disertacijos autoriaus nuomone, vieša vieta taip pat būtų galima apibrėžti viską, kas nepatenka į privačią erdvę. O kas Lietuvos teisėje laikoma privačia erdve oficialų paaiškinimą galima rasti tik Visuomenės informavimo įstatyme, kur pateiktas privataus gyvenimo apibrėžimas, jog nevieša erdve laikytina asmens, jo šeimos gyvenamoji aplinka, jai priklausanti privati teritorija ir kitos privačios patalpos, kurias asmuo naudoja savo ūkinei, komercinei ar profesinei veiklai[471]. Apytikrį vaizdą, kas laikoma privačia erdve, galima susidaryti iš situacijų LAT jurisprudencijoje. Čia neverta minėti bylų, kuriose ginčas kilo akivaizdžiai privačioje namų erdvėje, nes jose neatskleidžiamas viešosios ir privačios erdvės santykis. Tačiau verta aptarti bylas, kuriose kilo klausimas dėl to, ar ginčo erdvė buvo vieša ar privati, pvz., bylą, kurioje nudistų paplūdimius teismas buvo pripažinęs ne vieša, o nuošalia vieta[472]. Taip pat byla, kurioje vaizdo stebėjimo kameros buvo įrengtos ant daugiabučio namo išorės sienų. Šioje byloje teismas pripažino, kad daugiabučio namo įėjimai, kiemas, automobilių stovėjimo aikštelės taip pat nebūtų laikomos vieša vieta[473].

Analizuojant nors ir negausią LAT jurisprudenciją, kada atsakovai rėmėsi viešosios erdvės ribojimu (t. y. informaciją apie asmenį viešoje vietoje rinko be jo sutikimo), matyti, jog vien objektyvus faktas, kad asmens atvaizdas yra fiksuojamas viešojoje ar privačioje erdvėje, ne visuomet būna vienintelis kriterijus vertinant, ar tuo atveju buvo pažeistas privatumas. Tokių bylų, kuriose teismui užteko konstatuoti, jog atvaizdas buvo fiksuojamas viešoje vietoje, vos kelios. Pvz., byloje „J. B. v. VšĮ „Humana people to people Baltic" teismas motyvacinėje sprendimo dalyje išdėstyta, jog vieša darbo vieta nėra privati asmens sfera, o pardavėjo darbas yra viešo pobūdžio veikla, todėl darbuotojas negali reikalauti, kad jam būtų užtikrintas privatumas jo darbo vietoje, t. y. prekybos salėje, o pardavimo salės, kartu ir

467 LR triukšmo valdymo įstatymas, *Valstybės žinios,* 164, 5971 (2004), 6 straipsnio 1 punktas.

468 LR susirinkimų įstatymas, *Valstybės žinios,* 136, 6956 (2012), 4 straipsnio 1 dalis.

469 LAT Civilinių bylų skyriaus 2004 m. vasario 9 d. nutartis civilinėje byloje Nr. 3K-3-91.

470 LAT Civilinių bylų skyriaus 2004 m. gegužės 3 d. nutartis civilinėje byloje Nr. 3K-3-289.

471 Visuomenės informavimo įstatymo pakeitimo įstatymas, 2 straipsnio 40 dalis.

472 LAT Civilinių bylų skyriaus 2009 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-26/2009.

473 LAT Civilinių bylų skyriaus 2017 m. gruodžio 27 d. nutartis civilinėje byloje Nr. e3K-3-472-916/2017.

pardavėjo darbo, stebėjimas nėra slaptas asmens privataus gyvenimo stebėjimas[474]. Išimtinai teritorine viešosios ir privačios erdvės perskyra teismas motyvavo ir savo sprendimą byloje „D. M. ir L. M. v. UAB „Ekstra žinios“. Teismas konstatavo, jog nudistų paplūdimys laikytinas vieta, kuriai pripažintinas nuošalios, ne viešos, vietos statusas[475]. Pastebėtina, jog tokia teismo motyvacija labai artima privataus gyvenimo ribų suvokimui, kuris būdingas JAV teismams. Jų bylose esminę reikšmę sprendžiant dėl privatumo pažeidimo turi vertinimas, ar teritorinis stebėjimas vykdomas viešojoje ar privačioje erdvėje[476].

Lietuvos jurisprudencijoje nagrinėjama daugiau bylų, kuriose teismas atsižvelgia ne tik į aplinkybę, jog tariamas pažeidimas padarytas viešojoje ar privačioje erdvėje, bet ir į daugelį kitų kriterijų. Pvz., byloje „J. A. v. UAB „Lietuvos rytas“ teismas laikėsi nuomonės, jog asmuo gali nesutikti būti fotografuojamas net ir viešoje vietoje. Kitaip tariant, nors CK 2.22 straipsnio 2 dalis leidžia asmens atvaizdą viešoje vietoje fiksuoti be jo sutikimo, tačiau jeigu stebimasis aiškiai ir nedviprasmiškai išreiškė nenorą būti fotografuojamas, to turi būti paisoma. Tokiais atvejais svarbi subjektyvi vidinė fotografuojamo asmens nuostata[477]. Praktikoje pripažįstama, jog nesutikimas gali būti išreiškiamas tiek žodžiu, tiek raštu, tiek konkliudentiniais veiksmais (pvz., išreikštu nepasitenkinimu)[478]. Taigi vienas iš kriterijų, kada net ir viešoje vietoje filmuoti būtų negalima, yra tas, kai asmuo aiškiai ir nedviprasmiškai išreiškė nesutikimą. Šios praktikos LAT laikosi iki šiol[479].

Daugumoje bylų ginčai kyla tik tada, kai informacija apie asmenį arba jo atvaizdas būna viešai publikuojamas visuomenės informavimo priemonėse. Teismas tokiais atvejais pasisakė, jog nesutikimą būti filmuojamam reikėtų aiškinti ir kaip nesutikimą leisti transliuoti vaizdo įrašą per visuomenės

---

474 LAT Civilinių bylų skyriaus 2004 m. gegužės 3 d. nutartis civilinėje byloje Nr. 3K-3-289.

475 LAT Civilinių bylų skyriaus 2009 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-26/2009.

476 Disertacijos 3.2 poskyryje „Teorinis pagrindas reguliuojant privatumą viešojoje erdvėje“ šis požiūris vadinamas „dvinare teorija“, „viešosios ir privačios erdvės dichotomija“. Taip pat žr. bylas JAV teismų praktikoje, pvz., „California v. Greenwood“, 486 U.S. 35 (1988) (Teismas nusprendė, jog policija nepažeidė ketvirtosios pataisos įpareigodama šiukšlių surinkėją atskirti ieškovo šiukšles nuo kitų, kad šias policija galėtų vėliau apžiūrėti, nes ieškovo šiukšlės buvo viešoje vietoje.); „United States v. Scott“, 437 U.S. 82 (1978). (Teismas nusprendė, jog apgynė mokesčių inspekcijos agentų veiksmus – t. y., ieškovo šiukšlių konteineryje suradę susmulkintą popierių ir surinkę į įskaitomą dokumentą, nepažeidė ieškovo privatumo, nes ieškovo šiukšlių konteineris stovėjo viešoje vietoje).

477 LAT Civilinių bylų skyriaus 2004 m. vasario 9 d. nutartis civilinėje byloje Nr. 3K-3-91. (Byloje ginčas kilo, kai dienraštyje buvo išspausdintas straipsnis apie nuo AIDS mirusį vyrą. Straipsnyje aprašytos vyro užsikrėtimo aplinkybės, prie teksto buvo atspausdintos laidotuvių procesijos, kapo duobės nuotraukos. Į teismą kreipėsi velionio vyro žmona prašydama apginti jos ir velionio vyro teisę į privatų gyvenimą bei teisę į atvaizdą).

478 LAT Civilinių bylų skyriaus 2008 m. rugsėjo 23 d. nutartis civilinėje byloje Nr. 3K-3-394/2008.

479 Žr., pvz., LAT Civilinių bylų skyriaus 2020 m. spalio 28 d. nutartis civilinėje byloje Nr. e3K-3-278-403/2020. *Teismų praktika* 54 (2020): 11–24.

informavimo priemones[480]. Jei asmuo matydamas ir suvokdamas, kad yra filmuojamas, neišreiškia nesutikimo dėl filmuotos medžiagos transliavimo, tai nėra pagrindas vertinti, jog buvo duotas sutikimas filmuotą medžiagą transliuoti. Juolab kad filmuojamas asmuo negali žinoti, kokio turinio, apimties bus ši medžiaga, kaip ji bus sumontuota, kaip pateikta (paminint filmuoto asmens duomenis ar nepaminint, rodant jo veidą ar nerodant, komentuojant rodomą filmuotą medžiagą ar nekomentuojant)[481].

Pastebėtina, jog daugelis LAT nagrinėtų bylų yra susijusios būtent su atvaizdo fiksavimu ir vėlesniu jos publikavimu žiniasklaidoje. Ginčų, kuriuose informacija viešoje vietoje būtų surinkta, tačiau vėliau viešai nepublikuota, praktiškai nėra. Tikriausiai vienintelė tokia yra byla „R. M. v. A. L.“, kurioje ieškovas slapta įrašinėjo šalių pokalbį viešoje vietoje ir vėliau šį įrašą kaip įrodymą panaudojo teisme. Teismas vertinimą atliko vadovaudamasis tokiais kriterijais: 1) ar įrašas buvo daromas viešojoje ar privačioje erdvėje, 2) ar pasiklausomas asmuo kitai šaliai informaciją pokalbio metu teikė gera valia, t. y. ar nemelavo, 3) ar pasirinktas fiksavimo būdas ir apimtis nebuvo perteklinio masto, 4) ar įrašymo tikslas buvo pateisinamas siekiant apginti kitą pažeistą teisę[482]. Vis dėlto ginčų, kilusių dėl duomenų rinkimo, kai šie vėliau nebuvo publikuoti visuomenės informavimo priemonėse, Kasacinio teismo praktikoje nėra buvę, todėl ši praktika naujesnėse LAT bylose nėra išplėtota.

Valstybiniai subjektai asmens duomenis rinkdami viešoje vietoje gali vadovautis platesniu teisės į privatų gyvenimą ribojimu – visuomenės ir valstybės saugumo tikslu. Kasacinis teismas yra pasisakęs, jog „teisė į atvaizdą ir asmens privatumą gali būti ribojama valstybės saugumo, visuomenės saugos ir šalies ekonominės gerovės interesais, siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti; ribojimas būtinas demokratinėje visuomenėje, t. y. būtina sąlyga paskelbti informaciją apie privatų asmens gyvenimą be to asmens sutikimo yra tik teisėtas ir pagrįstas visuomenės interesas žinoti tokią informaciją, tačiau šio intereso negalima sutapatinti su tiesiog visuomenės interesu patenkinti savo smalsumą“[483]. Taigi vadovaujantis visuomenės ir valstybės saugumo tikslu valstybės institucijos gali be asmenų sutikimo rinkti duomenis tiek viešojoje, tiek privačioje erdvėje. Tačiau vertinant įsiveržimo proporcingumą viešojoje erdvėje, tikėtina, būtinumą pagrįsti būtų kur kas lengviau nei privačioje aplinkoje.

Kaip jau minėta ankstesniame poskyryje, EŽTT pateisina netgi masinę slaptą valstybės institucijų vykdomą stebėseną[484]. Tačiau kiek laisvės suteikiama

480 *Ibid.*

481 *Ibid.*

482 LAT Civilinių bylų skyriaus 2002 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 3K-3-1406. (Kasacinis teismas sprendė klausimą dėl garso įrašo, padaryto viešoje vietoje, priimtinumo kaip įrodymo byloje, nes jį ieškovas buvo padaręs slapta).

483 LAT 2008 m. rugsėjo 23 d. nutartį civilinėje byloje Nr. 3K-3-394/2008.

484 Žr. disertacijos 3.3.1 poskyrį.

žvalgybos institucijoms, susitariančios valstybės, tarp jų ir Lietuva, sprendžia nacionaliniu mastu. Vis dėlto Lietuvoje valstybės institucijų vykdoma stebėsena reglamentuota akivaizdžiai privatumo nenaudai. Masinę stebėseną reglamentuojantys teisės aktai Lietuvoje yra sulaukę Kasacinio teismo kritikos dėl neribotų stebėsenos terminų[485], o žvalgybą vykdantys pareigūnai dėl piktnaudžiavimo[486]. Teisės doktrinoje kritikuojama kriminalinės žvalgybos teisės aktuose neseniai atsiradusi „teisėsaugos institucijų užduoties" sąvoka, dėl kurios nepakankamo apibrėžtumo gali kilti grėsmė žmogaus teisių apsaugai[487].

Taigi, nors valstybėms suteikiama diskrecija masinę stebėseną riboti griežčiau negu reikalaujama pagal EŽTT praktiką, Lietuva šiuo metu žvalgybos institucijoms suteikia labai plačią diskreciją. Nors EŽTT dar nėra vertinęs Lietuvos žvalgybos režimo atitikties minimaliems standartams, suformuotiems „Big Brother Watch and Others v. the United Kingdom" byloje, kurie, kaip minėta, ir taip gana laisvi, yra manančių, jog Lietuvos teisės aktai neatitiktų ir jų[488].

---

485 LAT Baudžiamųjų bylų skyriaus 2015 m. birželio 1 d. nutartis baudžiamojoje byloje Nr. 2K-P-94-895/2015. *Teismų praktika,* 43, (2015): 476–465 („Kriminalinės žvalgybos įstatyme nors ir įtvirtinta, kad slapto asmenų pokalbių klausymosi bendras laikotarpis negali būti ilgesnis negu 12 mėnesių, tačiau kartu numatyti ir atvejai, kai šis laikotarpis gali būti neribotai pratęstas. Tačiau toks teisinis reguliavimas neatleidžia operatyvinės veiklos (kriminalinės žvalgybos) subjektų, prokurorų, teikiančių prašymus (teikimus) dėl šios operatyvinės (kriminalinės žvalgybos) priemonės taikymo, o teisėjų, priimančių sprendimus sankcionuoti tokių priemonių skyrimą (pratęsti jų taikymą), nuo pareigos įvertinti jos taikymo trukmės pagrįstumą ir proporcingumą. Netoleruotinos tokios teisinės situacijos, kai per protingą laiką nepasitvirtinus įtarimui dėl nusikalstamos veikos toliau nepagrįstai ilgai atliekama (sankcionuojama) slapta telekomunikacijų tinklais perduodamos informacijos turinio kontrolė iš esmės tikintis (nesant tam rimto pagrindo) gauti informacijos dėl kokios nors kitos nusikalstamos veikos ir taip siekiant pateisinti šios priemonės taikymą").

486 LAT Baudžiamųjų bylų skyriaus 2017 m. vasario 21 d. nutartis baudžiamojoje byloje Nr. 2K-57-696/2017, *Teismų praktika* 47, (2017): 540–554. („Šioje byloje į pirmiau išvardytus reikalavimus neatsižvelgta. Slaptos operatyvinių bei procesinės prievartos priemonės buvo pratęsiamos nenurodant pratęsimui reikalaujamų pagrindų, dėl to buvo pažeista proporcija tarp valstybės siekimo tikslo ir pasiekto rezultato. Teisėjų kolegija pažymi, kad netoleruotina, kai slapti operatyviniai ir procesiniai veiksmai pratęsinėjami, žmogaus privatus gyvenimas kontroliuojamas, nesurinkus naujos informacijos apie nusikalstamą veiką, o tik tikintis, kad jis galbūt vis vien kada padarys nusikaltimą, negaunant duomenų, patvirtinančių faktinį operatyvinių priemonių taikymo pagrindą, dėl kurio ir buvo sankcionuota pokalbių ir susižinojimo kontrolė").

487 Petras Tarasevičius, „Teisėsaugos institucijų užduotis kriminalinėje žvalgyboje", *Teisės problemos* 91, 1 (2016): 109.

488 Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu" (Vilnius: Mykolo Romerio universitetas, 2019, 70-71.

3.3.3. EŽTT ir Lietuvos privatumo viešojoje erdvėje jurisprudencijos vertinimas bepiločių orlaivių kontekste

Atlikus išsamią EŽTT ir Lietuvos jurisprudencijos, susijusios su privatumu viešojoje erdvėje, analizę vertėtų aptarti, kokią įtaką teismo suformuotos teisės taikymo taisyklės gali turėti sprendžiant privatumo problemas, kylančias dėl plataus masto nedidelių bepiločių orlaivių naudojimo. Kadangi analizuota praktika tiesiogiai nesusijusi su bepiločiais orlaiviais, esamoje jurisprudencijoje suformuotoms taisyklėms praplėsti disertacijos darbo autorius naudos ribų valdymo teoriją[489], kuri, kaip minėta, siūloma kaip pagrindas kurti naujus teisės aktus ir teismų praktikas. Nors nėra garantijų, jog teismų motyvacija šiame poskyryje iliustruojamais atvejais pasuktų būtent tokia linkme, tačiau manytina, jog mokslinis diskursas gali daryti poveikį teismų praktikos krypčiai.

Disertacijos autoriaus nuomone, Lietuvos jurisprudencija, susijusi su privatumu viešoje vietoje, yra labai nutolusi nuo problemų, kurias keltų nedidelių bepiločių orlaivių naudojimas. Joje nepakanka universalaus taikymo teisės taisyklių, todėl nuspėti Kasacinio teismo motyvaciją gali padėti nebent EŽTT praktika. Ji, manytina, suteikia aiškesnį vaizdą apie privatumo ribas viešojoje erdvėje bepiločių orlaivių naudojimo kontekste. CPK 3 straipsnio 6 dalis numato, kad Lietuvos teismai nagrinėdami bylas vadovaujasi, *inter alia*, ir EŽTT sprendimais, todėl disertacijos autorius toliau šiame poskyryje daugiau remiasi EŽTT jurisprudencijoje suformuotomis taisyklėmis.

Kaip jau minėta, bepiločiai orlaiviai stebėsenai vykdyti gali būti naudojami tiek valstybių, tiek didelę galią rinkoje turinčių privačių subjektų[490]. Analizuojant EŽTT bylas, nagrinėjančias privatumą viešojoje erdvėje, matyti, jog teismas privatumo viešoje vietoje ribas vertina skirtingai, tai priklauso nuo to, koks subjektas vykdo stebėjimą.

Kaip matyti iš atliktos analizės, kiek tai susiję su privatumo apsauga, tiek santykiuose tarp privačių subjektų, tiek tarp valstybės institucijų ir privačių asmenų, EŽTK pasirašiusioms valstybėms yra suteikiama diskrecija (angl. *margin of appreciation*) spręsti dėl konkrečių priemonių, kuriomis planuojama užtikrinti atitiktį EŽTK 8 straipsnio reikalavimams[491]. Vis dėlto lyginant kriterijus, kuriais EŽTT rekomenduoja nacionaliniu mastu užtikrinti asmenų privatumo apsaugą viešojoje erdvėje tarp privačių asmenų[492] ir tarp valstybės institucijų su privačiais asmenimis[493], panašu, kad susitariančių valstybių diskrecija mažesnė tais atvejuose, kai abi santykio šalys yra privačios.

---

489 Žr. disertacijos 3.2.3 poskyrį.

490 Žr. disertacijos 1.5.1 poskyrį.

491 „López Ribalda and Others v. Spain“ *supra note,* 146: 112; „Big Brother Watch and Others v. the United Kingdom“, *supra note,* 433: 340–342.

492 „López Ribalda and Others v. Spain“, *supra note,* 146: 116.

493 „Big Brother Watch and Others v. the United Kingdom”, *supra note,* 438: 335; „Weber and Saravia v. Germany (dec.)“, 95.

Bepiločių orlaivių kontekste tai reiškia, jog privačių subjektų bepiločiais orlaiviais vykdoma stebėsena turėtų būti griežčiau prižiūrima ir reguliuojama. Nors reikėtų, kad EŽTT plačiau išdėstytų nuomonę dėl EŽTK 8 straipsnio taikymo naujosioms vaizdo stebėjimo technologijoms[494], tačiau pritaikius ribų valdymo teoriją galima įvertinti, kokia būtų teismo nuomonė bepiločių orlaivių naudojimo atvejais, kai laikomasi jurisprudencijoje jau nustatytų taisyklių.

Pirma, EŽTT praktikoje suformuoti standartai suponuoja, jog viešoje vietoje skrydį planuojantys vykdyti bepiločių orlaivių valdytojai turėtų bent jau informuoti visus stebimuosius, kad planuoja juos filmuoti ir įrašyti jų duomenis. Palyginti su ICAO ir ES standartais, kurie numato ne tik informavimo, bet ir sutikimo gavimo pareigą[495], EŽTT reikalavimas būtų gana laisvas, suteiktų galimybę įgyvendinti griežtesnes priemones valstybių įstatymų leidėjams. Vis dėlto, kaip jau aptarta, net ir informavimo pareiga bepiločių orlaivių atveju gali būti sunkiai įgyvendinama praktiškai, jei skrydį vykdo vidutinis vartotojas[496].

Manytina, jog pagal EŽTT praktiką informavimo pareigos galima būtų nesilaikyti, jeigu bepiločiu orlaiviu viešoje vietoje asmenys tik filmuojami, tačiau įrašo duomenys nebūtų išsaugojami laikmenoje[497]. Tačiau tokią taisyklę teismas nustatė byloje, susijusioje su stebėjimu CCTV kameromis, kurios dažnai būna sujungtos laidais, todėl kelia mažesnę grėsmę *saugumo neužtikrinimo*[498] pažeidimo kontekste. Bepiločio orlaivio veikimas visiškai priklauso nuo bevielio duomenų ryšio, kuris susieja skirtingus jo komponentus, todėl visuomet egzistuoja tikimybė, jog bevieliu ryšiu perduodama informacija gali būti perimta ir įrašoma ne bepiločio orlaivio valdytojo, o trečiojo asmens (įsilaužėlio) duomenų laikmenoje.

Šiai jurisprudencijai iš esmės neprieštarauja ir BDAR numatyta išimtis, kuri įpareigoja informuoti ir gauti sutikimą, kai surinkti duomenys yra įrašomi, tačiau anonimizuojami[499]. Kitaip tariant, manytina, jog pagal EŽTT praktiką rinkti duomenis bepiločiu orlaiviu būtų teisėta be stebimųjų sutikimo, jeigu įrašyti duomenys būtų anonimizuojami. Vis dėlto anonimizavimo technologija turi imanentinių trūkumų, dėl kurių patikimai anonimizuoti duomenis šiuo metu neįmanoma[500].

Antra, EŽTT motyvacija bylose, susijusiose su privatumo viešojoje erdvėje, taip pat leidžia daryti išvadą, jog filmavimas bepiločiais orlaiviais viešoje vietoje turėtų būti leidžiamas, jeigu vykdomos stebėsenos mastas ir įsibrovimo į kitų asmenų privatų gyvenimą laipsnis nėra pernelyg didelis. Vertinant reikėtų atsižvelgti į privatumo lygį stebimoje srityje, taip pat į visus laiko ir erdvės apribojimus ir žmonių, turinčių prieigą prie stebėjimo rezultatų, skaičių.

---

494 „López Ribalda and Others v. Spain", supra note, 146: Joint dissenting opinion of judges De Gaetano, Yudkivska and Grozev 4.
495 Žr. disertacijos 2.3.2 poskyrį; disertacijos 4.2.1 poskyrį.
496 Žr. disertacijos 4.2.1 poskyrį.
497 Herbecq and the Association „Ligue Des Droits De L'homme v. Belgium (dec.)".
498 Žr. disertacijos 1.5.4 poskyrį.
499 Plačiau žr. disertacijos 4.2.1 poskyrį; BDAR, 4 straipsnio 5 dalis.
500 Žr. disertacijos 4.3.3 poskyrį.

Bepiločių orlaivių kontekste tai iš esmės reiškia, jog individualaus bepiločio orlaivio valdytojas turėtų susilaikyti nuo konkretaus asmens ar žmonių grupės nuolatinės stebėsenos, nes toks filmavimas netgi neįrašant vaizdo į išorinę laikmeną, tikėtina, būtų traktuojamas kaip pernelyg įkyrus. Taip pat turėtų vengti vykdyti skrydžius tokiose vietose, kurios, netgi būdamos viešoje vietoje, iš prigimties yra privačios, pvz., nudistų pliažuose, persirengimo kabinose, tualetuose. Individualūs bepiločių orlaivių valdytojai taip pat turėtų pastebėti, kokius ribų valdymo mechanizmus naudoja stebimi individai. Kaip jau minėta, siekdami nustatyti ribas viešojoje erdvėje žmonės gali naudoti įvairius aplinkos daiktus, tokius kaip durys ir sienos[501]. Todėl jei asmuo viešoje vietoje yra sąmoningai atsiskyręs siena, pertvarka, durimis ar kitokiu objektu, tikėtina, jog jis nori būti vienas ir nustebtų sužinojęs, jog buvo filmuojamas bepiločiu orlaiviu. Taigi manytina, jog tokį stebėjimą teismas turėtų vertinti kaip privatumo pažeidimą.

Taip pat jau buvo minėta, jog žmonės riboms sukurti gali naudoti ir neverbalinius ženklus[502] (rankų kryžiavimą, mojavimą, veido išraiškas), kuriais, pvz., gali reikšti nepasitenkinimą, kad individualaus bepiločio orlaivio valdytojas vykdo skrydį. Tikėtina, jog stebimųjų rodomi neverbaliniai ženklai savaime nesukeltų bepiločio orlaivio valdytojui pareigos nutraukti skrydį, jeigu šiems prieš tai būtų suteikta galimybė keisti savo elgesį, t. y. jeigu juos bepiločio orlaivio valdytojas informuotų apie skrydį iš anksto. Keisti savo elgesį stebimieji taip pat galėtų, jeigu valstybė iš esmės toleruoja tokius skrydžius atitinkamoje viešosios erdvės vietoje ir yra informavusi valstybės piliečius iš anksto. Šį sprendimą, disertacijos darbo autoriaus nuomone, vertėtų aptarti detaliau.

Remiantis ribų valdymo teorija, visuomenės elgesio modeliai, kuriuos valstybė nori išsaugoti (ar slopinti), galiausiai turėtų būti įtvirtinti teisės aktais, kad visuomenei būtų aišku, kokiomis aplinkybėmis viešoje vietoje reikia keisti savo elgesį[503], o kitiems suinteresuotiems subjektams būtų aišku, kokiomis aplinkybėmis galima vykdyti skrydžius, rinkti ir įrašyti informaciją apie individus.

Tobulėjant stebėsenos technologijoms riba tarp virtualios ir realios erdvės neišvengiamai nyksta, todėl reikėtų nustatyti, jog tam tikros viešosios erdvės vietos yra visiškai atviros stebėsenai, kitose stebėsena draudžiama, o trečiose, galbūt, būtų priimtina ribota stebėsena. Pvz., įstatymų leidėjai galėtų priimti teisės aktus, leidžiančius nuolatinę pagrindinės miesto aikštės ar pėsčiųjų gatvės atkarpos stebėseną. Šiose viešosiose erdvėse bepiločių orlaivių skrydžiai galėtų būti vykdomi be apribojimų[504], komercines paslaugas teikiantys asmenys galėtų rinkti ir agreguoti duomenis apie vartotojus, nes šie būtų iš anksto informuoti apie būtent toje viešoje

501 Žr. disertacijos 3.2.3 poskyrį.
502 *Ibid.*
503 *Ibid.*
504 Turima omenyje, jog be apribojimų skrydžiai galėtų būti vykdomi, kiek tai susiję su privatumo apsauga. Be abejo, dronų valdytojai turėtų laikytis visų saugumo reikalavimų, kurie nepatenka į šios disertacijos tyrimo sritį.

vietoje vykstančia nuolatinę stebėseną[505]. Iš EŽTT perspektyvos, pagal kurį, kaip minėta, turėtų užtekti informavimo pareigos, toks susitariančios valstybės sprendimas turėtų neišeiti iš jos diskrecijos ribų. Pagal ES duomenų apsaugos teisę toks reguliavimas taip pat turėtų būti priimtinas[506]. Galimas ir alternatyvus sprendimas, tačiau jis labai priklausytų nuo anonimizavimo ir RFID technologijų pažangos bei patikimumo. Disertacijos autoriaus nuomone, asmenys, kurie nori būti matomi aktyviai stebimose viešosios erdvės vietose, galėtų nešioti RFID žymas, kurios bepiločiams orlaiviams transliuotų sutikimo dalyvauti nuostatą (angl. *opt-in*), o visų kitų asmenų, neišreiškusių sutikimo, duomenys galėtų būti anonimizuojami preziumuojant, jog itin pažangi technologija rinką pasieks ateityje[507].

Trečia, vertinant EŽTT jurisprudencijoje nustatytas taisykles, manytina, jog bepiločio orlaivio valdytojas turėtų turėti aiškų teisinį pagrindą, pateisinantį stebėjimą ir jo mastą – kuo įkyresnis stebėjimas, tuo stipresnis turėtų būti pagrindimas. Taip pat turėtų įvertinti, ar stebėsenos tikslas negali būti įgyvendintas mažiau landžiais metodais ir priemonėmis, įvertinti pasekmes, kurias gali sukelti vykdoma stebėsena. Negana to, stebimiems asmenims turėtų būti suteiktos pakankamos apsaugos priemonės.

Kaip jau aptarta aukščiau, geriausią teisinį pagrindą suteiktų teisės aktu įtvirtintas ribų valdymo mechanizmas, pagal kurį visuomenei būtų aišku, kada reikia keisti savo elgesį, o kada galima jaustis laisviau, nes bepiločiais orlaiviais aktyvi stebėsena nevykdoma. Disertacijos autoriaus vertinimu, vienas tokių ribų valdymo mechanizmų, aptartų aukščiau, galėtų būti leidimas vykdyti neribotą stebėseną tam tikrose viešosios erdvės vietose, o kitose – jos visiškas draudimas, išskyrus siauras išimtis, kurios galėtų būti numatytos įstatymuose.

Į tokių teisės aktų rengimo procesą turėtų būti įtraukiami visuomenės ir įvairių rinkų atstovai, kad būtų gan detaliai įvertinama, ar tokia stebėsena atitinkamu atveju būtina, ar stebimiems asmenims būtų suteikiamos pakankamos apsaugos priemonės. Manytina, jog tokiu atveju našta sureguliuoti santykius, susijusius su privatumo apsauga bepiločių orlaivių kontekste, pagrįstai tektų ne didelę galią rinkoje turintiems privatiems subjektams, o valstybei, kuri objektyviausiai, kiek tai įmanoma demokratinėje visuomenėje, gali nuspręsti, kuriuos elgesio modelius reikia išsaugoti, o kuriuos galima prislopinti dėl didesnio gėrio.

Toliau vertėtų aptarti, kaip vertintina EŽTT ir Lietuvos teismų praktika dėl privatumo apsaugos bepiločių orlaivių kontekste, kai stebėseną viešoje vietoje vykdo valdžios institucijos. Vėlgi bylos, kurias EŽTT ir Lietuvos teismai nagrinėjo iki šiol, nebuvo tiesiogiai susijusios su bepiločiais orlaiviais, bet iš jų galima susidaro aiškų vaizdą, kokios pozicijos teismas laikytųsi, jei valdžios institucijos stebėseną vykdytų bepiločiais orlaiviais.

---

505 Apie šį pasiūlymą plačiau žr. disertacijos 4.6 poskyrį.
506 Žr. disertacijos 4.2.3 poskyrį.
507 Žr. disertacijos 4.3.3 poskyrį.

„Big Brother Watch and Others v. the United Kingdom“ byloje teisėjų kolegijos dauguma iš esmės nukreipė tarptautinę justiciją privatumui nepalankia linkme ir leido valstybei masinę stebėseną vykdyti praktiškai neribotai, neatsižvelgiant į tai, kokiomis priemonėmis duomenys renkami. Taigi bepiločius orlaivius, kaip vieną iš informacijos rinkimo priemonių, valstybės galėtų slapta naudoti beveik be apribojimų. Tiesa, įstatymų leidėjai turėtų įtvirtinti tam tikras procedūrines garantijas, kurios minimizuotų valstybės kišimąsi į privatų gyvenimą, tačiau, atsižvelgiant į kontroversiškas atskirąsias nuomones išdėsčiusių EŽTT teisėjų nuomones, vargu ar teismo nustatytus procedūrinius kriterijus galima laikyti pakankama materialine privatumo apsauga[508]. Lietuvos teisės aktai, nepaisant teismų kritikos, šiuo metu suka keliu, kuris nepalankus privatumui[509].

Slapta masinė stebėsena, kad ir kas ją vykdo – valdžios institucijos ar privatūs asmenys, iš materialiosios teisės perspektyvos būtų nesuderinama su ribų valdymo teorija, tai tik didintų privatumo pažeidimų skaičių, nes asmenys, nežinodami, kad yra stebimi, negali keisti savo elgesio. Kaip jau minėta, jei visuomenė bus įsitikinusi, jog yra stebima visur ir visada, tai gali lemti atšalimo efektą[510]. Šiuo aspektu reikia sutikti su M. Žalnieryte, jog tarptautinė justicija pakrypo pavojinga kryptimi[511], kurią, disertacijos autoriaus nuomone, pakeisti galima būtų politine valia atsisakant valdžios institucijų vykdomos masinės stebėsenos. Šia linkme rekomenduotina eiti ir Lietuvos teisės aktų leidėjams.

508 „Big Brother Watch and Others v. the United Kingdom“, *supra note,* 438: Joint partly dissenting opinion of judges Lemmens, Ranzoni and Bošnjak; Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque.

509 Žr. disertacijos 3.3.2 poskyrį.

510 Žr. disertacijos 1.5.1 poskyrį.

511 Zalnieriute, „Big Brother Watch and Others v. the United Kingdom“, *supra note,* 455.

4. BEPILOČIAI ORLAIVIAI IR DUOMENŲ APSAUGA

Duomenų apsauga yra svarbi teisės į privatumą dalis, ypač dabar, kai pažangiomis technologijomis duomenis gali rinkti dideliais kiekiais, juos automatiškai perduoti ir agreguoti. Kaip jau minėta, bepiločiai orlaiviai kelia grėsmę duomenų apsaugai, nes jais naudojantis galima surinkti didžiulį informacijos kiekį[512]. Bepiločiai orlaiviai gali prisidėti ir prie tokių duomenų apdorojimo pažeidimų kaip agregavimas, identifikavimas ir saugumo neužtikrinimas[513]. ES duomenų apsaugą užtikrina BDAR[514], todėl disertacijoje bus analizuojamas šis dokumentas tiek, kiek jis siejasi su bepiločių orlaivių naudojimu. Šis skyrius įgyvendina penktą ir šeštą uždavinius.

Pirmame poskyryje aptariama, kaip BDAR taikomas bepiločiams orlaiviams. Antrajame apibrėžiami duomenų rinkimo pagrindai. Trečiajame – analizuojamos BDAR siūlomos privatumo apsaugos priemonės ir vertinama, ar jos suteikia pakankamą privatumo apsaugą nuo grėsmių, kylančių vis plačiau naudojant bepiločius orlaivius. Penktame poskyryje aptariami dabartinės, sutikimu paremtos privatumo apsaugos sistemos trūkumai. Šeštajame pateikiami disertacijos autoriaus siūlymai dėl privatumo reguliavimo ateityje.

Svarbu pažymėti, kad šeštajame poskyryje nebuvo siekiama detalizuoti galimų teisės aktų struktūros ar formuluočių. Disertacijos tikslas – išanalizuoti esamą bepiločių orlaivių naudojimo privatumo reguliavimą bei specialųjį bepiločių orlaivių reguliavimą ir pateikti jų tobulinimo pasiūlymus. Dėl nuolatinės technologinės pažangos ir kintančios teisinės aplinkos pernelyg konkretus teisės aktų modeliavimas galėtų apriboti šių pasiūlymų lankstumą bei apsunkinti jų pritaikomumą skirtinguose kontekstuose. Dėl šios priežasties disertacijoje akcentuojamas reguliavimo principų ir jų taikymo krypčių formavimas, o ne specifinių teisės normų formulavimas. Šis požiūris leidžia išlaikyti pusiausvyrą tarp privatumo apsaugos ir bepiločių orlaivių technologinės plėtros, suteikiant erdvės teisėkūros institucijoms ir rinkos dalyviams pritaikyti siūlomas gaires prie besikeičiančių aplinkybių. Toks metodas taip pat užtikrina, kad siūlomi sprendimai būtų pakankamai lankstūs ir neapsunkintų inovacijų diegimo, kartu stiprinant teisinį aiškumą ir užkertant kelią galimam piktnaudžiavimui.

4.1. Kaip BDAR taikomas naudojant bepiločius orlaivius

Pirmiausia vertėtų apsibrėžti, kaip BDAR taikomas bepiločių orlaivių skrydžiams. Reglamentas yra taikomas asmens duomenų tvarkymui, o duomenų tvarkymas suprantamas, kaip „bet kokia automatizuotomis arba neautomatizuotomis

512 Žr. disertacijos 1.5.2 poskyrį.
513 Žr. disertacijos 1 skyrių.
514 BDAR.
515 „BDAR, 2 straipsnio 1 dalis.

priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis“[516]. Bepiločiai orlaiviai yra informacijos rinkimo priemonės, todėl formaliai į BDAR materialinę taikymo sritį patenka.

Vis dėlto BDAR numato ir tam tikras išimtis. BDAR būtų taikomas tik tuo atveju, jeigu bepiločiu orlaiviu surinkta informacija būtų traktuojama kaip „asmens duomenys“. Pagal apibrėžimą tai „bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti“[517]. Tuo tarpu fizinio asmens tapatybę galima nustatyti pagal fizinės, fiziologinės, genetinės, psichinės, ekonominės ar socialinės tapatybės požymius[518]. Taigi tam, kad būtų taikomas BDAR, iš bepiločiu orlaiviu surinktų duomenų turėtų būti įmanoma nustatyti asmens tapatybę. Svarbu paminėti, jog prie asmens duomenų BDAR priskiria ir duomenis, kurie buvo pseudonimizuoti[519]. Tačiau anonimizuoti duomenys[520] į BDAR taikymo sritį nepatektų[521], nes iš jų identifikuoti konkretų asmenį turėtų būti neįmanoma.

Išimtis galima tada, kai duomenis tvarko fizinis asmuo, užsiimantis išimtinai asmenine ar namų ūkio veikla[522]. BDAR 2 straipsnio 2 dalies c punktas numato, kad reglamentas nėra taikomas, kai duomenų tvarkymas atliekamas grynai asmeniniais ar buitiniais tikslais. Todėl formaliai BDAR neturėtų būti taikomas bepiločių orlaivių skrydžiams, kurie vykdomi fizinių asmenų pramoginiais tikslais, pavyzdžiui, asmeniniam naudojimui filmuojant gamtovaizdžius ar šeimos šventes. Vis dėlto, šios išimties taikymo ribos nėra absoliučios. ESTT yra patikslinęs, kad

---

516 *Ibid.,* 4 straipsnio 2 punktas.

517 BDAR, 4 straipsnio 1 punktas.

518 *Ibid.*

519 BDAR pseudonimų suteikimas suprantamas kaip asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti. BDAR, 4 straipsnio 5 punktas, preambulės 26 punktas.

520 BDAR anonimišką informaciją apibrėžia kaip informaciją, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta. BDAR, preambulės 26 punktas.

521 *Ibid.*

522 *Ibid.,* 2 straipsnio 2 dalies c punktas.

„asmeninės ar namų ūkio veiklos išimtis“ negali būti taikoma, kai asmens duomenys renkami viešosiose erdvėse, net jei tai daro privatus asmuo[523]. Tokia jurisprudencija buvo suformuota dar prieš bepiločių orlaivių technologijų išpopuliarėjimą, tačiau ji gali turėti įtakos aiškinant BDAR taikymo ribas dronų naudojimo kontekste. Jei būtų laikomasi šios logikos, BDAR reikalavimai galėtų būti taikomi visiems bepiločių orlaivių skrydžiams viešojoje erdvėje, nepriklausomai nuo to, ar juos vykdo privatūs asmenys, ar organizacijos.

Vis dėlto, toks aiškinimas kelia tam tikrų abejonių. Disertacijos autoriaus nuomone, būtų neproporcinga ir nepraktiška BDAR atitikties naštą užkrauti kiekvienam fiziniam asmeniui, kuris pramoginiais tikslais skraidina bepiločius orlaivius viešose vietose, ypač atsižvelgiant į tai, kad šie asmenys dažniausiai nesiekia sistemingai rinkti ar analizuoti asmens duomenų. Tokia reguliavimo našta galėtų pernelyg suvaržyti bepiločių orlaivių naudojimą nekomerciniais tikslais, o tai prieštarautų proporcingumo principui, kuris yra vienas pagrindinių ES teisės principų. Be to, praktikoje bepiločių orlaivių skrydžiai ne visuomet reiškia asmens duomenų tvarkymą BDAR prasme. Dėl šios priežasties išlieka neaišku, ar ESTT laikytųsi tokios pat griežtos pozicijos bepiločių orlaivių kontekste, kaip ir kitais atvejais, kai buvo aiškinama „asmeninės ar namų ūkio veiklos“ išimties apimtis. Atsižvelgiant į šiuos aspektus, tikslesnis BDAR taikymo bepiločių orlaivių naudojimui aiškinimas galėtų būti plėtojamas per ateities ESTT jurisprudenciją arba specializuotus duomenų apsaugos priežiūros institucijų išaiškinimus.

Kita išimtis galima tada, kai „duomenis tvarko kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais“[524]. Todėl BDAR taip pat netaikomas, kai skrydžius bepiločiu orlaiviu vykdo valdžios institucijos bandydamos užtikrinti nacionalinį saugumą ar užkirsti kelią nusikaltimams.

Dar svarbu paminėti, jog BDAR taikomas bet kokioms technologijoms, kuriomis tvarkomi asmens duomenys, ne tik bepiločiams orlaiviams, apie kuriuos konkrečių užuominų BDAR tekste nerasime. Todėl BDAR siūlomos apsaugos priemonės dažniausiai yra labai abstrakčios, paliekančios gana didelę diskreciją valstybių narių įstatymų leidžiamajai valdžiai, teismams bei rinkos žaidėjams. Dėl plačios BDAR apimties disertacijoje atliekama analizė bus apribota (i) duomenų rinkimo bepiločiais orlaiviais pagrindais bei (ii) pagrindinėmis privatumo apsaugos priemonėmis, kurias siūlo BDAR.

---

523 Žr. disertacijos 4.2.1 poskyrį; Case C-212/13 on CCTV http://curia.europa.eu/juris/document/document.jsf?text=95%252F46%252FEC&docid=160561&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=300923#ctx1.

524 BDAR, 2 straipsnio 2 dalies d punktas.

4.2. Duomenų rinkimo bepiločiais orlaiviais pagrindai

Toliau galima pereiti prie pagrindų, kuriais vadovaujantis duomenų rinkimas bepiločiu orlaiviu būtų teisėtas pagal BDAR. Tokius atvejus numato BDAR 6 straipsnis:

a) gautas duomenų subjekto sutikimas;

b) rinkti duomenis būtina siekiant įvykdyti sutartį;

c) rinkti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė;

d) rinkti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus;

e) rinkti duomenis būtina viešojo intereso labui;

f) rinkti duomenis būtina vadovaujantis teisėtu interesu[525].

Disertacijos autoriaus nuomone, detaliai aptarti b, c, d ir e pagrindų nebūtina, nes bepiločių orlaivių kontekste iš jų reikšmingų problemų nekyla. Vis dėlto klausimų gali kilti kalbant apie a ir f.

Vienas iš teikiamų siūlymų yra bepiločių orlaivių naudojimą reguliuoti vadovaujantis ribų valdymo teorija, pagal kurią duomenų tvarkymą privatūs subjektai vykdytų nacionalinio teisės akto pagrindu[526]. BDAR 6 straipsnis *expressis verbis* tokio duomenų tvarkymo pagrindo nenumato, todėl taip pat reikėtų panagrinėti, ar taikyti disertacijos autoriaus siūlymą būtų teisėta pagal BDAR.

4.2.1. Sutikimas kaip pagrindas rinkti duomenis bepiločiu orlaiviu

Konkrečiau vertinant a pagrindą (t. y. BDAR 6 straipsnio 1 dalies a punktas), esminis neaiškumas yra tas, ar visais atvejais vykdant skrydžius bepiločiu orlaiviu viešoje vietoje būtina gauti aplinkinių asmenų sutikimą. Siekiant atsakyti į šį klausimą vertėtų detaliau panagrinėti BDAR reikalavimus sutikimui.

BDAR kelia tokius pagrindinius reikalavimus: 1) sutikimas turi būti duotas laisva valia, 2) sutikimas turi būti konkretus, 3) sutikimas turi būti pagrįstas informacija, 4) sutikimas turi būti nedviprasmiškas, 5) duomenų valdytojas gali įrodyti sutikimo gavimą, 6) duomenų subjektui turi būti suteikta galimybė bet kada savo sutikimą atšaukti. Tam tikrais išimtiniais atvejais iš duomenų subjekto gali būti privaloma gauti 7) aiškų sutikimą (angl. *explicit consent*)[527]. Vertėtų išsiaiškinti kiekvieno iš šių reikalavimų turinį ir panagrinėti, kaip jie būtų pritaikomi duomenų tvarkymui vykdant bepiločių orlaivių skrydžius.

(1) *Laisva valia duotas* sutikimas iš esmės reiškia, kad duomenų subjekui

525 BDAR, 6 straipsnio 1 dalis.

526 Žr. disertacijos 3.2.3 poskyrį ir 4.6 poskyrį.

527 „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, Europos duomenų apsaugos valdyba, 2020-05-04.

suteikta reali sprendžiamoji galia, t. y. asmuo gali pasirinkti duoti ar neduoti sutikimą dėl duomenų tvarkymo ir dėl to nepatirti jokių neigiamų pasekmių[528]. Nustatant, ar sutikimas buvo duotas laisva valia BDAR nurodomi keli *prima facie* atvejai, kada laisvos valios kriterijus būtų laikomas pažeistu. Tarp jų, pvz., (i) *galios disbalansas* – kai yra aiškus duomenų subjekto ir duomenų valdytojo padėties disbalansas, ypač kai duomenų valdytojas yra valdžios institucija[529]; (ii) *sąlygų nustatymas* – kai sutikimas tvarkyti duomenis reikalaujamas kaip sąlyga norint naudotis paslauga, nors tie duomenys nėra būtini paslaugai teikti[530]; (iii) *detalumas* – kai neleidžiama duoti atskiro sutikimo atskiroms asmens duomenų tvarkymo operacijoms, nors tai ir tikslinga atskirais atvejais[531]; (iv) *žala* – kai duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti nepatirdamas žalos[532]. Kiekvieną atvejį vertėtų aptarti kiek detaliau.

BDAR aiškiai nurodo, jog dėl (i) *galios disbalanso* sutikimu kaip duomenų tvarkymo pagrindu valdžios institucijos vadovautis neturėtų. Vis dėlto gali pasitaikyti atvejų, kada ir valdžios institucija šiuo pagrindu vadovautis galėtų[533]. Galios disbalansas gali atsirasti ir su darbo santykiais susijusiuose kontekstuose, todėl remtis sutikimu kaip duomenų tvarkymo pagrindu darbdavys galėtų tik išimtinėmis aplinkybėmis[534]. Neskaitant situacijų, susijusių su valdžios institucijomis

528 „Rekomendacija smulkiajam ir vidutiniam verslui dėl Bendrojo duomenų apsaugos reglamento taikymo“, VDAI, 2018-09-05, https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacijos_smulkiajam%20ir%20vidutiniam%20verslui%20del%20BDAR%20taikymo%202018-09-05.pdf.

529 BDAR, preambulės 43 punktas; „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 8.

530 BDAR, 7 straipsnis 4 dalis, preambulės 43 punktas; „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 10.

531 BDAR, 7 straipsnis 4 dalis, preambulės 43 punktas; „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 10.

532 BDAR, preambulės 42 punktas; „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 13.

533 „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, supra note, 531: 8. (Gairėse pateikiamas pavyzdys: „Nuosavos žemės turinčiam asmeniui reikia gauti tam tikrus savo vietos savivaldybės ir provincijos, kurioje yra ta savivaldybė, valdžios leidimus. Abiem viešosioms institucijoms reikia tos pačios informacijos, kad galėtų išduoti leidimą, tačiau jos neturi prieigos prie viena kitos duomenų bazių. Todėl jos abi prašo pateikti tą pačią informaciją ir žemės savininkė nusiunčia savo duomenis abiem valdžios institucijoms. Savivaldybė ir provincijos valdžios institucija prašo jos sutikimo, kad jos dokumentų bylos būtų sujungtos, todėl nereikėtų dubliuoti procedūrų ir korespondencijos. Abi valdžios institucijos patikina, kad tai neprivaloma ir kad jeigu ji nuspręs nesutikti su savo duomenų sujungimu, jos prašymai išduoti leidimus bus vis vien nagrinėjami atskirai. Žemės savininkė gali laisva valia duoti sutikimą šioms institucijoms, kad jos dokumentų bylos būtų sujungtos“).

534 Ibid., 8. (Gairėse pateiktas pavyzdys: „Filmo kūrėjų grupė ketina filmuoti tam tikroje biuro patalpų dalyje. Darbdavys prašo visų darbuotojų, kurių sėdimos darbo vietos yra toje zonoje, sutikimo, kad būtų filmuojami, nes jie gali būti matomi vaizdo įrašo antrame plane. Tie, kurie nenori būti filmuojami, už tai niekaip nebaudžiami ir jiems skiriami lygiaverčiai darbo stalai kitose pastato dalyse iki filmavimo pabaigos“).

arba darbo santykiais, galios disbalansas gali atsirasti ir kitomis aplinkybėmis, kai duomenų subjektas rizikuoja patirti apgaulę, bauginimą, prievartą ar reikšmingų neigiamų pasekmių (pvz., nemažų papildomų išlaidų), jei sutikimo neduotų[535].

(ii) *Sąlygų nustatymas* kaip laisva valia duoto sutikimo sudedamoji dalis reiškia, jog sutikimas neatskiriamai sujungiamas su kitomis sąlygomis, su kuriomis nebūtina sutikti, arba kai su sutarties vykdymu ar paslaugos teikimu yra susiejamas prašymas duoti sutikimą duomenų tvarkymui, nors tie duomenys nėra būtini įvykdyti sutarčiai ar teikti paslaugai. Kai duomenys tvarkomi siekiant įvykdyti sutartį, sutikimas apskritai nebūtų reikalingas, nes tokiu atveju paslaugų teikėjas duomenis gali tvarkyti BDAR 6 straipsnio 1 dalies b punkto pagrindu (sutartis). Kita vertus, sutartis gali numatyti, kad prašomi duomenys nėra būtini sutarčiai vykdyti (įskaitant paslaugos teikimą), tačiau ta sutartis bus vykdoma tik su sąlyga, kad duomenų subjekto sutikimo pagrindu bus gauti nebūtini duomenys. Tokiu atveju duomenų subjekto sutikimas nebūtų traktuojamas kaip duotas laisva valia, t. y. tokios sąlygos sutartyje nebūtų teisėtos pagal BDAR[536].

Kita laisvai duoto sutikimo sąlyga yra (iii) *detalumas,* kuris pasireiškia, kai teikiant paslaugą atliekamos kelios duomenų tvarkymo operacijos siekiant ne vieno, o daugiau tikslų. Tokiu atveju duomenų subjektas turėtų turėti laisvę rinktis, su kuriais tikslais sutinka, o su kuriais – ne, t. y. iš duomenų subjekto negalima reikalauti sutikti su visu duomenų tvarkymo tikslų rinkiniu, nesuteikiant galimybės pareikšti sutikimų dėl kiekvieno atskiro tikslo. Taigi, kai duomenys tvarkomi siekiant kelių tikslų, duomenų valdytojas privalo sutikimą detalizuoti, kad duomenų subjektas galėtų pareikšti savo sutikimą (nesutikimą) dėl kiekvieno tikslo atskirai[537].

Laisva valia duoto sutikimo (iv) *žalos* kriterijus suponuoja duomenų valdytojo pareigą įrodyti, jog duomenų subjektas gali atsisakyti sutikti su duomenų tvarkymu arba atšauti savo sutikimą nepatirdamas žalos (pvz., papildomų išlaidų, nepalankių sąlygų, apgaulės, bauginimo, prievartos ar kitų reikšmingų neigiamų pasekmių)[538].

Pagal BDAR sutikimas taip pat turi būti (2) *konkretus*. Ši sąlyga vartotojui suteikia daugiau kontrolės, o sutikimui daugiau skaidrumo. Ji veikia kaip apsaugos

---

535 *Ibid.,* 9.

536 *Ibid.,* 10–12.

537 *Ibid.,* 12–13.

538 *Ibid.,* 13 (gairėse įvardijama, pvz., tokia situacija, kuri lemtų žalos duomenų subjektui atsiradimą: „Parsisiunčiant mobiliąją gyvenimo būdo programėlę prašoma sutikimo, kad joje būtų naudojami telefono akcelerometro (pagreičio matuoklio) duomenys. Tai nėra būtina šios programėlės veikimui, tačiau tai naudinga duomenų valdytojui, kuris nori daugiau sužinoti apie savo programėlės naudotojų judėjimą ir aktyvumą. Viena naudotoja vėliau atšaukia duotą sutikimą ir pastebi, kad programėlės veikimas nuo to laiko yra apribotas. Tai yra tokios žalos, apie kurią kalbama 42 konstatuojamojoje dalyje, pavyzdys, kuris reiškia, kad gautas sutikimas niekada nebuvo galiojantis (todėl duomenų valdytojas turi ištrinti visus taip surinktus asmens duomenis apie programėlės naudotojų judėjimą“).

priemonė nuo laipsniško duomenų tvarkymo tikslų plėtimo arba suliejimo po to, kai duomenų subjektas sutinka su pradiniu duomenų rinkimu, dar vadinamu nemotyvuotu nukrypimu nuo funkcijų (angl. *function creep*). Konkretumas neatsiejamas nuo kitų sutikimo kriterijų ir iš esmės reiškia, kad turi būti konkrečiai nurodomi duomenų tvarkymo tikslai, kiekvienam tikslui turėtų būti atskiras konkretus prašymas duoti sutikimą. Informacija, susijusi su duomenų tvarkymu, taip pat turėtų būti aiškiai atskiriama nuo informacijos, susijusios su kitais dalykais. Duomenų subjektas duodamas sutikimą atitinkamu atveju privalo suprasti, kad jis kontroliuoja padėtį ir kad jo duomenys bus tvarkomi tik siekiant nustatytų tikslų[539].

(3) *Informacija pagrįstas sutikimas* reiškia, kad duomenų subjektui privaloma suteikti visą reikalingą informaciją iš anksto, kad jis suprastų, su kuo sutinka. Pasak EDAV, kad sutikimas būtų pagrįstas informacija, duomenų subjektui reikėtų pateikti: duomenų valdytojo tapatybę; kiekvienos iš duomenų tvarkymo operacijų tikslą; kokios rūšies duomenys bus renkami ir kam naudojami, informuojama apie jo turimą teisę atšaukti sutikimą; informaciją apie duomenų naudojimą automatizuotam sprendimų priėmimui (pvz., agregavimui, profiliavimui); informaciją apie galimą duomenų perdavimo riziką. Informacija duomenų subjektui gali būti pateikta įvairiais būdais: rašytiniu, žodiniu pareiškimu, garso ar vaizdo pranešimais. Pranešimas turėtų būti suformuluotas aiškia ir paprasta kalba, kad jį suprastų ne tik teisininkams, bet ir paprastas žmogus, t. y. vengti ilgų, sudėtingų privatumo politikos tekstų ar pareiškimų, kuriuose daug teisinių terminų[540].

Informacija pagrįstas sutikimas taip pat reiškia, jog svarbi informacija negali būti „paslėpta" bendrose sąlygose. Bepiločių orlaivių kontekste įmanomas scenarijus, kada didelę galią rinkoje turintis duomenų valdytojas, teikiantis įvairias paslaugas internete, sutikimą duomenis rinkti bepiločiu orlaiviu gali gauti slapta. Daugelis duomenų valdytojų interneto svetainėse vartotojams pateikia sutikimo formas, kurias išvydę jie dažniausiai spaudžia mygtuką „sutikti", nors gali rinktis ir „nesutikti"[541]. Prie šio reiškinio prisideda ir patys duomenų valdytojai[542]. Ateityje

539 Ibid., 14–15. (Pvz.: „Kabelinės televizijos tinklas renka savo abonentų asmens duomenis remdamasis jų sutikimu, kad galėtų teikti jiems asmeninius pasiūlymus, kokie nauji filmai galėtų juos dominti, sprendžiant iš jų televizijos žiūrėjimo įpročių. Vėliau tas televizijos tinklas nusprendžia, kad norėtų leisti trečiosioms šalims siųsti (arba rodyti ekrane) tikslinę reklamą, parinktą pagal abonento televizijos žiūrėjimo įpročius. Dėl šio naujo tikslo reikia naujo sutikimo").

540 Ibid., 15–18.

541 Anna Pastore, „Consent Notices and Cognitive Cost after the GDPR : An Experimental Study" (masterThesis, 2020), https://repositorio.ucp.pt/handle/10400.14/31285 (atliktas elgsenos tyrimas parodė, jog net jeigu žmonėms pateikiami pasirinkimai „sutikti su visais" ir „nesutikti su visais", jie labiau linkę spausti „sutikti su visais").

542 Anna Pastore, „Consent Notices and Cognitive Cost after the GDPR : An Experimental Study" (masterThesis, 2020), https://repositorio.ucp.pt/handle/10400.14/31285 (atliktas elgsenos tyrimas parodė, jog net jeigu žmonėms pateikiami pasirinkimai „sutikti su visais" ir „nesutikti su visais", jie labiau linkę spausti „sutikti su visais").

gali rastis situacijų, kai į tokias masinio sutikimo formas bus įtrauktas ir duomenų tvarkymas bepiločiais orlaiviais. Vartotojas, nepaspaudęs internetinės duomenų valdytojo tvarkymo politikos nuorodos arba „valdyti nustatymus“, gali net nežinoti, jog į sutikimo formą įtrauktas ir sutikimas duomenis rinkti bepiločiais orlaiviais. Esant tokiai situacijai, didžiųjų duomenų valdytojams būtų suteikta galimybė vykdyti masinę stebėseną bepiločiais orlaiviais, prisidengiant sutikimu kaip teisiniu pagrindu duomenims tvarkyti. Nors sutikimas dėl stebėsenos bepiločiu orlaiviu, kuris įtrauktas į interneto svetainės privatumo politiką, neatitiktų konteksto, kur vartotojas galėtų tikėtis tokios sąlygos. Kažin ar tokį sutikimą galima būtų laikyti informatyviu. Kita vertus, netolimoje ateityje privatumo politika tikriausiai bus vertinama pasitelkiant dirbtinį intelektą, dėl to tokias sąlygas bus sunkiau nuslėpti[543].

Pagal BDAR sutikimas turi būti (4) *nedviprasmiškas*. Tai reiškia sutikimo dalyvauti nuostatą (angl. *opt-in*), kuri reikalauja aktyvių duomenų subjekto veiksmų. Kitaip sakant, asmens tylėjimas ar neveikimas, taip pat iš anksto pažymėti langeliai ar bet koks kitas numanomo sutikimo būdas neturėtų būti laikomas sutikimu. Sutikimas gali būti išreiškiamas ne tik žodžiu ar raštu, bet ir fiziniais duomenų subjekto veiksmais. Bepiločių orlaivių skrydžių vykdymo kontekste tai reiškia, jog sutikimą (nesutikimą) galima būtų gauti ir, pvz., atitinkamą reikšmę turinčiu rankos mostu, tačiau tokiu atveju duomenų subjektas turėtų būti tinkamai informuotas apie sutikimą ar nesutikimą išreiškiančius ženklus bei jų reikšmes.

Duomenų valdytojas turi turėti (5) *galimybę įrodyti, jog gavo duomenų subjekto sutikimą.* BDAR tiksliai nenustato, kaip tai turėtų būti įgyvendinta, bet EDAV siūlo, pvz., saugoti įrašus apie gautus sutikimo pareiškimus, taip tap informaciją apie vartotojo seansą internetinėje aplinkoje, per kurį buvo išreikštas sutikimas, kartu su dokumentais apie visą sutikimo eigą ir informacijos kopija, pateikta duomenų subjektui. Vien nurodyti atitinkamos svetainės sandarą nepakaktų. BDAR nenumato, kiek galiotų sutikimas. Tai turėtų būti vertinama *ad hoc*. Tačiau susidarius situacijai, kai duomenų tvarkymo operacijos reikšmingai pasikeitė, pradinis sutikimas nebegaliotų ir reikėtų gauti naują[544].

Svarbu ir tai, kad duomenų subjektas turėtų (6) galimybę sutikimą atšaukti. Duomenų valdytojas turėtų užtikrinti, kad sutikimą bus galima atšaukti taip pat lengvai, kaip jį duoti. Tai reiškia, kad duomenų subjektas turėtų gebėti atšaukti savo sutikimą nepatirdamas žalos (turi būti suteikta galimybė sutikimą atšaukti nemokamai, neprastinant teikiamų paslaugų lygio). Kai duomenys tvarkomi ir pagal sutartį, ir pagal sutikimą, duomenų valdytojas turėtų nuo pat pradžių aiškiai nustatyti, kuris pagrindas taikytinas atitinkamai duomenų grupei, kad vėliau duomenų subjektui atšaukus sutikimą duomenų valdytojas galėtų ištrinti

543 Giuseppe Contissa ir kt., „Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence“, *SSRN Electronic Journal,* 2018 m. sausio 1 d., https://doi.org/10.2139/ssrn.3208596.

544 „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 23–24.

būtent tuos duomenis, kuriuos tvarkė sutikimo pagrindu. Kai duomenų subjektas atšaukia savo sutikimą, tačiau duomenų valdytojas nori toliau tvarkyti jo duomenis remdamasis kitu teisėtu pagrindu, jis privalo apie tai pranešti duomenų subjektui[545].

Galiausiai BDAR numato tam tikras duomenų tvarkymo kategorijas, kada būtų reikalingas (7) *aiškus sutikimas* (angl. *explicit consent*). Tai jautrūs duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose, taip pat genetiniai biometriniai duomenys, iš kurių siekiama konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją[546]. Aiškus sutikimas taip pat reikalingas, kai duomenys perduodami į trečiąsias valstybes arba tarptautinėms organizacijoms, kai nesilaikoma BDAR 49 straipsnyje nurodytų apsaugos priemonių[547]. Taip pat tais atvejais, jeigu duomenis planuojama apdoroti automatizuotomis priemonėmis, profiliuoti[548].

Aiškus sutikimas nuo įprasto sutikimo skiriasi išraiška. Iš esmės tiek vienas, tiek kitas gali būti duodami žodžiu ir raštu, tačiau aiškus sutikimas jau nebegalėtų būti išreiškiamas vien veiksmais (pvz., bepiločių orlaivių atveju – rankos mostu, kaip aptarta kiek aukščiau). EDAV rekomenduoja tokius sutikimus gauti kartu su duomenų subjekto parašu. Kaip aiškus sutikimas būtų traktuojami atvejai, kai duomenų subjektas užpildo elektroninę formą, išsiunčia el. laišką, skanuotą ar el. parašu pasirašytą sutikimą duomenų valdytojui. Galima gauti sutikimą ir telefonu, jei informacija yra sąžiningai bei suprantamai pateikiama apie galimybę rinktis ir duomenų subjekto paprašoma konkretaus patvirtinimo (pvz., pateikti patvirtinimą žodžiu ar paspausti mygtuką). Dviejų etapų autentifikacijos metodai taip pat užtikrintų, kad būtų laikomasi aiškiam sutikimui keliamų reikalavimų[549].

Detaliai panagrinėjus reikalavimus sutikimui pagal BDAR, sunku įsivaizduoti, kaip viešoje vietoje skrydį vykdantis vidutinis vartotojas galėtų jų laikytis. Fizinis asmuo, valdantis nedidelį bepilotį orlaivį, net nedisponuoja ištekliais, kurių reikia dideliu mastu pranešti apie skrydį, nekalbant apie visas sutikimo subtilybes, nurodomas BDAR. Todėl tikėtina, kad BDAR taikymas fiziniams asmenims, skraidinantiems bepiločius orlaivius nekomerciniais tikslais, turėtų būti aiškinamas kitaip nei ankstesnėse ESTT bylose dėl stebėjimo viešoje vietoje.

Kaip minėta ankstesniame poskyryje (žr. 4.1), ESTT yra išaiškinęs, kad „asmeninės ar namų ūkio veiklos“ išimtis negalioja, kai asmens duomenys renkami viešojoje erdvėje. Jei šis aiškinimas būtų tiesiogiai pritaikytas bepiločių orlaivių naudotojams, reikštų, kad net ir pramoginiais tikslais skraidinantys fiziniai asmenys būtų įpareigoti laikytis visų BDAR reikalavimų, įskaitant pareigą gauti aplinkinių asmenų sutikimą. Tokiu atveju vidutiniai vartotojai, siekdami išvengti galimų teisinių pasekmių, galėtų vykdyti skrydžius nebent tokiose vietose, kur pašalinių

545 *Ibid.,* 24–26.
546 BDAR, 9 straipsnis.
547 „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 21.
548 BDAR, 22 straipsnis.
549 „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, *supra note,* 531: 22.

asmenų nėra arba jų yra labai mažai. Taip pat jiems tektų imtis papildomų atsargumo priemonių – skraidinti bepiločius orlaivius tokiu atstumu, iš kurio žmonių identifikavimas neįmanomas, arba užtikrinti, kad vaizdo įrašai nebūtų išsaugomi[550].

Tačiau toks aiškinimas gali būti laikomas per griežtu bepiločių orlaivių kontekste. Skirtingai nei vaizdo stebėjimo sistemos, kurios dažnai naudojamos sisteminiam asmenų sekimui, individualių naudotojų vykdomi bepiločių orlaivių skrydžiai dažniausiai neturi tokio masto ar tikslingumo. Todėl tikslingiau būtų atsižvelgti į faktinį stebėsenos pobūdį ir intensyvumą, o ne vien į tai, kad skrydžiai vykdomi viešose vietose. Jei vietoje tiesioginio ESTT praktikos taikymo būtų pripažinta, kad fiziniai asmenys paprastai nesiekia sistemingai rinkti asmens duomenų, jų veiklai BDAR galėtų būti taikomas lankstesnis reguliavimas.

Tačiau net ir atleidus individualius naudotojus nuo griežtų BDAR reikalavimų, tam tikros privatumo pažeidimo rizikos išliktų aktualios. Viena iš tokių rizikų – saugumo neužtikrinimas[551], kai surinkti duomenys būtų saugomi nesaugiose laikmenose ir galėtų tapti kibernetinių atakų taikiniu. Vis dėlto, kadangi fizinių asmenų namų ūkio poreikiais naudojami bepiločiai orlaiviai dažniausiai nefiksuoja sistemingos, didelės apimties ar ypatingai jautrios informacijos apie stebimus asmenis, tokia grėsmė išlieka labiau teorinė.

Kita galima rizika – vadinamasis atidengimo[552] pažeidimas, kai asmeniui kyla psichologinis diskomfortas žinant, jog jis buvo nufilmuotas. Pavyzdžiui, jei bepiločio orlaivio vaizdo kamera fiksuoja žmogų kompromituojančioje situacijoje (pvz., paplūdimio persirengimo kabinoje), net jei tokia medžiaga nėra viešai paskelbiama, pats suvokimas, kad ji egzistuoja, gali sukelti nerimą dėl galimos ateities grėsmės. Tokie privatumo pažeidimai gali būti sprendžiami taikant papildomas prevencines priemones. Viena iš galimų išeičių – sukurti centralizuotą skrydžių registrą, prieinamą tik valstybės institucijoms, kuriame būtų fiksuojamos bepiločių orlaivių valdytojų vykdomų skrydžių geografinės koordinatės, laikas ir data[553]. Kaip jau minėta ankstesniame disertacijos skyriuje, toks reikalavimas padėtų užtikrinti pusiausvyrą tarp asmenų privatumo ir bepiločių orlaivių naudotojų teisių[554]. Šiuo metu ES specialusis bepiločių orlaivių reguliavimas numato tik vietinį duomenų transliavimą[555], kuris nėra toks veiksmingas.

---

550 Žr. disertacijos 4.2.1 poskyrį; disertacijos 4.3.3 poskyrį.

551 Žr. disertacijos 1.5.4 poskyrį.

552 Žr. disertacijos 1.5.5 poskyrį.

553 Žr. disertacijos 2.3.7 poskyrį (Panaši nuostata buvo numatyta JAV FAA nuotolinių identifikavimo priedų reguliavimo pasiūlyme, pagal kurį bepilotis orlaivis skrydžio metu realiu laiku internetu FAA įgaliotai bendrovei privalo perduoti tiek savo geografinę padėtį, tiek ir laiko žymą. Vis dėlto FAA nusprendė šios nuostatos į galutinį nuotolinių identifikavimo priedų reguliavimą neįtraukti tokios nuostatos neįtraukti teisės akto derinimo su visuomene stadijoje išaiškėjus daug techninių pasiūlymo trūkumų, dėl kurių šiuo metu įgyvendinti tokį reikalavimą būtų sudėtinga.)

554 Žr. disertacijos 2.3.7 poskyrį.

555 Reglamento (ES) 2019/947 priedo 6 dalis, taip pat žr. disertacijos 2.3.7 poskyrį.

Dar viena išeitis galėtų būti anonimizavimo technologiniai sprendimai – tokiais metodais apdoroti duomenys į BDAR taikymo sritį nepatektų. Vis dėlto, disertacijos autoriaus vertinimu, toks sprendimas iš esmės nebūtų veiksmingas atidengimo atvejais. Atidengimo pažeidimas pasireiškia pirmiausia psichologinio skausmo sukėlimu stebimajam vien dėl to, kad šis žino, jog kažkas jį stebėjo – anonimizavimas nuo šio pažeidimo aspekto niekaip neapsaugotų. Išvestinės atidengimo pasekmės, pvz., vėlesnis nuotraukų publikavimas ar šantažas, gali sukelti dar didesnę stebėsenos aukos kančią – ar nuo šio pažeidimo aspekto anonimizavimas apsaugotų, priklauso nuo pačios anonimizavimo technologijos galimybių[556].

Vykdant komercinės paskirties skrydžius gauti BDAR reikalavimus atitinkantį sutikimą bepiločių orlaivių valdytojams turėtų būti paprasčiau, nes asmenis, kuriuos gali paveikti vykdomas skrydis, apibrėžti lengviau. Taip pat komercinius skrydžius vykdantys subjektai disponuoja pakankamais ištekliais ir didesniu mastu gali pranešti apie planuojamą skrydį, parengti reikalingus dokumentus ir sutikimo formuluotes, atitinkančias BDAR. Tačiau net ir vykdant komercinį skrydį sutikimą ne visada paprasta gauti. Komercinius bepiločių skrydžius pagal tikslą galima būtų skirstyti į dvi grupes, kurių: 1) tiesioginis skrydžio tikslas yra tvarkyti asmens duomenis (pvz., stebėti konkrečius asmenis ar teritoriją, fiksuoti mobiliųjų telefonų duomenų ryšį ir pan.); 2) skrydžio tikslas *a priori* tiesiogiai nesusijęs su asmens duomenų tvarkymu, bet tam tikrais atvejais turėti įtakos pašalinių asmenų teisei į privatumą (pvz., infrastruktūros apžiūros, topografiniai tyrimai, kitos fotografijos ir vaizdo įrašų paslaugos).

Pirmosios grupės skrydžiai privatumui kelia didesnę grėsmę, nes jų metu surinkta informacija apie skrydžio teritorijoje esančius individus būtų labai išsami. Taip pat tikėtina, jog tokių duomenų tvarkymas būtų naudojamas BDAR 22 straipsnyje nurodytais tikslais[557], o tokiam duomenų tvarkymui visuomet būtų reikalingas aiškus sutikimas. Tokio skrydžio atveju sutikimą bepiločio orlaivio valdytojui turėtų būti įmanoma gauti, jeigu renkami duomenys nėra pernelyg asmeniški, duomenų rinkimo tikslas nėra per daug ambicingas ir renkami labai konkrečiai apibrėžtų asmenų, kurie gali susipažinti su renkamų duomenų turiniu gerokai prieš skrydį, duomenys, pvz., įsigydami bilietą į renginį. Tačiau manytina, kad šios grupės skrydžiams sutikimas nėra pats geriausias pagrindas vykdyti skrydį. Jeigu renginio dalyvis, pvz., išreikštų nesutikimą, kad būtų tvarkomi jo asmens duomenys, tokiam asmeniui bet kokiu atveju turėtų būti leidžiama dalyvauti renginyje pagal sutartį, bet filmavimas ar kitų duomenų rinkimas bepiločiu orlaiviu renginio metu daugeliu atvejų būtų nebūtina sutarties įvykdymo sąlyga, todėl jam turėtų būti reikalingas atskiras duomenų subjekto sutikimas. Tačiau, bent vienam

---

556 Kad anonimizavimas būtų veiksmingas apsaugai nuo šio atidengimo pažeidimo aspekto, priklausytų ir nuo to, ar anonimizuojamas tik stebimojo veidas ar ir kūnas, ar anonimizuojama namų aplinka, kiemas ir pan.

557 BDAR, 9 straipsnis „Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą“.

asmeniui nesutikus, pakelti bepilotį orlaivį į orą nelieka teisinio pagrindo. Tokiu atveju skrydį būtų galima vykdyti tik kitais 6 straipsnyje numatytais pagrindais arba pasitelkiant technologinius sprendimus, kurie leistų nedavusių sutikimo individų duomenis realiu laiku anonimizuoti, t. y. kol duomenys neįrašyti į bepiločio orlaivio atminties kortelę.

Vykdant skrydžius, kurių tikslas *a priori* nėra susijęs su asmens duomenų tvarkymu, yra kiek paprasčiau, nes paveiktus asmenis tokios operacijos atveju žymiai lengviau apibrėžti. Pvz., pristatant siuntinį sutikimą tvarkyti asmens duomenis užtektų duoti pirkėjui, į kurio žemės sklypą pristatoma siunta, nes bepilotis orlaivis visą skrydį galėtų vykdyti dideliame aukštyje ir tik pasiekęs teritoriją, kurioje reikia palikti siuntinį, sumažintų savo altitudę. Kildamas ir leisdamasis bepilotis gali užfiksuoti ir nesusijusių su misija duomenų, pvz., tai, kas vyksta aplinkiniame rajone, tačiau užfiksuotų duomenų jautrumas, tikėtina, būtų minimalus. Panašų sprendimą jau yra aprašę E. Bassi ir kt.[558], kurie siūlo BDAR reikalavimus atitinkančios interaktyvių žemėlapių paslaugos, panašios į „Google maps“, tik pritaikytos būtent bepiločių orlaivių naudojimui, karkasą. Dar vienas tokių skrydžių pavyzdys galėtų būti nekilnojamojo turto ar kitų objektų apžiūros, kur net pageidautinas pašalinių asmenų nedalyvavimas kadre, todėl asmenų, kurių sutikimus reikėtų gauti, būtų labai nedaug, o užfiksuojamų asmens duomenų, vykdant tokius skrydžius, būtų nedaug. Be to, surinktos medžiagos turinys tikriausiai nebūtų įdomus asmens duomenis kaupiantiems ir interpretuojantiems subjektams. Vienintelis atvejis, kada galėtų kilti problemų gaunant sutikimą, yra, kai skrydis vykdomas viešoje vietoje fotografijos tikslais, atsitiktinėmis aplinkybėmis arba didelių renginių metu ir iš tokio nedidelio atstumo, kad galima būtų identifikuoti kadre esančius asmenis. Tokiu atveju sutikimą gauti būtų praktiškai neįmanoma, o skrydį būtų galima vykdyti tik kitais BDAR 6 straipsnyje numatytais pagrindais.

4.2.2. Teisėtas interesas kaip pagrindas rinkti duomenis bepiločiu orlaiviu

Pereinant prie BDAR 6 straipsnio 1 dalies f punkte nurodyto pagrindo, neaiškumų kyla dėl formuluotės abstraktumo[559], dėl kurio didžiųjų duomenų valdytojams atsirastų galimybė piktnaudžiauti. Vertėtų pasiaiškinti, kokioms situacijoms susidarius būtų pripažįstama, jog bepiločiu orlaiviu vykdomas duomenų rinkimas atitinka „teisėto intereso“ kriterijų ir ar abstrakti teisės akto formuluotė

558 Eleonora Bassi ir kt., „The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management“, *Minds and Machines* 29, 4 (2019): 579–601.

559 Tiksli formuluotė nurodyta BDAR 6 straipsnio 1 dalies f punkte yra: „Tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas.“

nesuteikia didelę galią rinkoje turintiems subjektams pernelyg plačių teisių rinkti ir toliau tvarkyti surinktus duomenis.

Šis teisinis pagrindas išskiria tuo, kad nėra orientuotas į konkretų tikslą (pvz., sutarties su asmeniu vykdymą, teisinės pareigos laikymąsi, gyvybinių interesų apsaugą, viešojo intereso apsaugą). Juo vadovaujantis, renkant duomenis bepiločiu orlaiviu, iš duomenų subjekto nereikėtų gauti sutikimo[560]. Keli *prima facie* teisėtų interesų pavyzdžiai, kurie būtų viršesni už duomenų subjektų interesus, pateikiami BDAR preambulėje. Tarp jų asmens duomenų tvarkymas sukčiavimo prevencijos tikslais (BDAR preambulės 47 punktas), tiesioginės rinkodaros tikslais (BDAR preambulės 47 punktas), vidaus administraciniais tikslais (BDAR preambulės 48 punktas) bei tinklo ir informacijos saugumo užtikrinimo tikslais (BDAR preambulės 49 punktas). Bepiločių orlaivių kontekste aktualus galėtų būti nebent asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, o visi kiti BDAR preambulėje nurodyti „teisėto intereso" pavyzdžiai, atrodo, nelabai pritaikomi.

BDAR preambulės 47 punkte nurodoma, kad „asmens duomenų tvarkymas tiesioginės rinkodaros tikslais gali būti vertinamas kaip atliekamas vadovaujantis teisėtu interesu". Iš šios nuostatos reikėtų suprasti, jog BDAR asmens duomenų tvarkymas tiesioginės rinkodaros tikslais suprantamas kaip tvarkymas, kuris vykdomas vadovaujantis teisėtu tikslu, todėl iš pirmo žvilgsnio duomenų subjekto sutikimas tokiu atveju neturėtų būti reikalingas. Kitaip tariant, panašu, jog duomenų valdytojas pagal BDAR gali tvarkyti duomenų subjekto duomenis negavęs jo sutikimo, o duomenų subjektui suteikiama teisė paprieštarauti tokiam duomenų tvarkymui, t. y. pasinaudoti atsisakymo dalyvauti nuostata (angl. *opt-out*). Vis dėlto reikalavimą gauti sutikimą, leidžiantį rinkti duomenis rinkodaros tikslais, (sutikimo dalyvauti nuostatą) numato kitas teisės aktas – Direktyva 2002/58/EB[561], kurią Lietuvoje įgyvendina Elektroninių ryšių įstatymas[562]. Jeigu bepiločiai orlaiviai skrisdami renka informaciją tiesioginės rinkodaros tikslais, duomenų subjektų sutikimo būtinai reikėtų ne pagal BDAR, o pagal Elektroninių ryšių įstatymą.

Dėl teisėto intereso pagrindo taikymo yra pasisakęs ir ESTT[563]. Teismo

---

560 „Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį", 29 straipsnio duomenų apsaugos darbo grupė, 844/14/LT, WP 217 (2014).

561 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) su paskutiniais pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB.

562 LR elektroninių ryšių įstatymas, *supra note,* 181.

563 Žr. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado, No. Joined cases C-468/10 and C-469/10 (ECJ 2011 m. lapkričio 24 d.); Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, No. Case C-131/12 (ECJ 2014 m. gegužės 13 d.); Patrick Breyer v. Bundesrepublik Deutschland, No. Case C-582/14 (ECJ 2016 m. spalio 19 d.); Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme", No. Case C-13/16 (ECJ 2017 m. gegužės 4 d.).

vertinant, ar duomenys pagal teisėtų interesų pagrindą buvo tvarkomi teisėtai, būtina įvertinti tris dalykus: t. y., pirma, ar duomenų tvarkytojo interesas gali būti kvalifikuojamas kaip teisėtas; antra, ar atitinkamu atveju buvo būtina tvarkyti asmens duomenis; trečia, ar buvo tinkama pusiausvyra tarp priešingų teisių ir interesų[564]. Panašu, jog teisėto intereso duomenų tvarkymo pagrindo turinio ESTT sąmoningai atskleisti nepageidauja ir pasilieka teisę dėl jo taikymo kiekvienąsyk spręsti *ad hoc,* nes išsamesnio aiškinimo nei pateiktas sprendimuose nerasime.

Detaliau apie teisėto intereso pagrindo taikymą yra pasisakiusi 29 straipsnio duomenų apsaugos darbo grupė (šiuo metu – Europos duomenų apsaugos valdyba[565]). Tiesa, vertėtų paminėti, jog darbo grupė komentuoja ne BDAR 6 straipsnį, o beveik analogišką nuostatą iš Duomenų apsaugos direktyvos[566], kuri buvo taikoma prieš įsigaliojant BDAR. Pasak darbo grupės, interesą galima laikyti teisėtu, jeigu duomenų valdytojas gali jo siekti nepažeisdamas duomenų apsaugos ir kitų teisės aktų, t. y. jis turi būti priimtinas pagal teisės normas[567]. Baigtinio tokių teisėtų interesų sąrašo nėra, bet kaip pavyzdžius darbo grupė pateikia:

Duomenų paskelbimą skaidrumo ir atskaitomybės tikslais. Pasak darbo grupės, duomenys viešai atskleidžiami visų pirma ne dėl duomenų valdytojo, kuris juos paskelbia, interesų, o todėl, kad tai atitinka kitų suinteresuotųjų subjektų, kuriems tie duomenys atskleidžiami, pvz., darbuotojų, žurnalistų ar plačiosios visuomenės interesus.

Istorijos arba kitų sričių mokslinius tyrimus. Pasak darbo grupės, vykdant mokslinius tyrimus gali reikėti gauti prieigą prie tam tikrų duomenų bazių.

Plačiosios visuomenės interesą arba trečiosios šalies interesą. Tokie atvejai gali pasitaikyti, kai duomenų valdytojas siekia intereso, atitinkančio plačiosios visuomenės ar trečiosios šalies interesą (gali būti raginamas ir, pvz., valdžios institucijų). Tai dažniausiai būna pagalba teisėsaugos tarnyboms ar privatiems subjektams kovoti su neteisėta veikla, tokia kaip pinigų plovimas, vaikų viliojimas ar neteisėtas keitimasis failais internetu[568].

Disertacijos autoriaus vertinimu, atsižvelgiant į darbo grupės aiškinimą, į „teisėto intereso" duomenų tvarkymą iš esmės įeitų ir bepiločių orlaivių naudojimas žurnalistikos, mokslo tyrimų, neteisėtos veikos išaiškinimo tikslais, taip pat

---

564 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme".

565 Po Bendrojo duomenų apsaugos reglamento įsigaliojimo 2015 m. gegužės 25 d. 29 straipsnio duomenų apsaugos darbo grupės funkcijas iš esmės perėmė Europos duomenų apsaugos valdyba (angl. *European Data Protection Board*). „Article 29 Working Party | European Data Protection Board", žiūrėta 2022 m. lapkričio 14 d., https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en.

566 „1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo", 13, 015 DD § (1995), http://data.europa.eu/eli/dir/1995/46/oj/lit.

567 „Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį", *supra note,* 564: 25.

568 *Ibid.,* 28–29.

tais atvejais, kurių BDAR rengėjai neturėjo galimybės numatyti teisės akto priėmimo momentu, siekiant teisės aktui suteikti atsparumą ateičiai.

Vertinant, ar „teisėto intereso“ duomenų tvarkymo tikslas nesuteikia dingsčių didžiųjų duomenų valdytojams piktnaudžiauti abstrakčia šios normos formuluote, disertacijos autoriaus manymu, tai mažai tikėtina. Nors duomenų tvarkymo pagal teisėto intereso pagrindą sąrašas nėra baigtinis, bet manytina, jog daugelis jų būtų teismo vertinami balansuojant asmens teisę į asmens duomenų apsaugą su saviraiškos laisve[569]. Didžiųjų duomenų valdytojai bando rasti nematomas elgesio struktūras visuomenėje, kad galėtų parduoti kuo daugiau prekių ir paslaugų, kas iš esmės beveik visuomet reiškia, jog duomenys bus tvarkomi tiesioginės rinkodaros tikslais, o šiam tikslui yra būtinas duomenų subjekto sutikimas pagal elektroninių ryšių privatumą reglamentuojančius teisės aktus. Taip pat abejotina, jog teismai „teisėto intereso“ pagrindą, kaip įtraukiantį duomenų tvarkymą tiesioginės rinkodaros tikslais, galėtų aiškinti plečiamai.

4.2.3. Nacionalinis teisės aktas kaip pagrindas duomenis rinkti bepiločiu orlaiviu

Disertacijoje siūloma bepiločių orlaivių naudojimą reguliuoti vadovaujantis ribų valdymo teorija[570], pagal kurią iš jų valdytojo nebūtų reikalaujama gauti sutikimą duomenų tvarkymui iš stebimų asmenų. Pagrindas tvarkyti asmens duomenis, taikant disertacijos autoriaus siūlomą reguliavimo modelį, privatiems subjektams turėtų būti privalomo pobūdžio nacionalinis teisės aktas, kuris nustatytų atitinkamą viešojoje erdvėje taikomą ribų valdymo mechanizmą. BDAR *expressis verbis* asmens duomenims tvarkyti tokio pagrindo nenumato, tačiau tam tikrą diskreciją išplėsti numatytuosius pagrindus valstybėms narėms suteikia BDAR 6 straipsnio 2 dalis. Vertėtų panagrinėti, ar pagal šią nuostatą nacionalinis teisės aktas galėtų būti asmens duomenų tvarkymo pagrindas privatiems duomenų valdytojams.

BDAR 6 straipsnio 2 dalyje nurodoma:

Valstybės narės gali toliau taikyti arba nustatyti konkretesnes nuostatas šio reglamento taisyklių taikymui pritaikyti, kiek tai susiję su duomenų tvarkymu, kad būtų laikomasi 1 dalies c ir e punktų, tiksliau nustatydamos konkrečius duomenų tvarkymui keliamus reikalavimus ir kitas teisėto ir sąžiningo duomenų tvarkymo užtikrinimo priemones, įskaitant kitais specialiais IX skyriuje numatytais duomenų tvarkymo atvejais.

569 ES saviraiškos laisvė lygmeniu įtvirtinta, pvz., EŽTK 10 straipsnyje.
570 Žr. disertacijos 3.2.3 poskyrį ir 4.6 poskyrį.

Disertacijos autoriaus vertinimu, pagal šią nuostatą valstybės narės gali priimti naujus nacionalinius teisės aktus arba palikti galioti jau esamus, kuriais kai kurie duomenų tvarkymo pagrindai būtų labiau detalizuoti. Vis dėlto žodžiai „konkretesnes" ir „tiksliau" nurodyti normos dispozicijoje reiškia, jog nacionaliniais teisės aktais nustatomi pagrindai neturėtų būti nauji, t. y. jie tik detaliau aptartų tam tikrus BDAR numatytus asmens duomenų tvarkymo pagrindus. Konkrečiau reglamentuoti šalims leidžiama BDAR 6 straipsnio 2 dalies c punkte („tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė") ir 6 straipsnio 2 dalies e punkte („tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas") nurodytus asmens duomenų tvarkymo pagrindus. Iš esmės tai patvirtina ir BDAR preambulės 8 punktas, nustatantis, jog „šiuo reglamentu numatoma galimybė valstybės narės teisėje konkrečiau apibrėžti reglamento taisykles ar numatyti jų apribojimus, valstybės narės, kiek tai būtina suderinamumui užtikrinti ir siekiant, kad nacionalinės nuostatos būtų suprantamos asmenims, kuriems jos taikomos, gali į savo nacionalinę teisę įtraukti šio reglamento elementus". Ir BDAR preambulės 9 punktas, kuriame pripažįstama, jog duomenų apsaugos reikalavimai tarp bendrijos šalių gali šiek tiek skirtis dėl nevienodo Direktyvos 95/46/EB įgyvendinimo.

Panašu, jog BDAR 6 straipsnio 3 dalies b punktas konkretizuoja, kokius reikalavimus turėtų atitikti toks nacionalinis reguliavimas. *Pirma,* detalizuojant BDAR 6 straipsnio 2 dalies c punkte nurodytą pagrindą, nacionalinis reguliavimas turėtų nustatyto duomenų tvarkymo tikslą, o detalizuojant pagal BDAR 6 straipsnio 2 dalies e punktą, tikslas turėtų būti – atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas. *Antra,* nacionaliniais teisės aktais nustatytas duomenų tvarkymo pagrindas taip pat galėtų išdėstyti konkrečias nuostatas, kaip pritaikyti BDAR taisykles. Tokios galėtų būti, *inter alia,* bendrosios sąlygos, reglamentuojančios duomenų valdytojo atliekamo duomenų tvarkymo teisėtumą; tvarkytinų duomenų rūšys; atitinkami duomenų subjektai; subjektai, kuriems asmens duomenys gali būti atskleisti, ir tikslai, dėl kurių asmens duomenys gali būti atskleisti; tikslo apribojimo principas; saugojimo laikotarpiai ir duomenų tvarkymo operacijos bei duomenų tvarkymo procedūros, įskaitant priemones, kuriomis būtų užtikrintas teisėtas ir sąžiningas duomenų tvarkymas, kaip antai tos, kurios yra skirtos kitiems, IX skyriuje numatytiems duomenų tvarkymo atvejams. *Trečia,* nacionalinės nuostatos turėtų atitikti viešojo intereso tikslą ir būti proporcingos teisėtam tikslui. Vis dėlto, disertacijos autoriaus vertinimu, ši nuostata praktiškai nepadeda aiškinant BDAR 6 straipsnio 2 dalį, nes joje iš esmės tik abstrakčiai primenama, jog nacionaliniai teisės aktai turi pernelyg nenukrypti nuo BDAR reikalavimų. Kiti tyrėjai pripažįsta, kad BDAR 6 straipsnio 3 dalis BDAR 6 straipsnio 2 dalies atžvilgiu perteklinė[571].

571 Julian Wagner ir Alexander Benecke, „National Legislation within the Framework of the GDPR", *European Data Protection Law Review (EDPL)* 2, 3 (2016): 353–61.

Nors atsakyti į šio poskyrio pradžioje iškeltą klausimą iš padarytos analizės būtų sunku, visgi platesnio aiškinimo nerasime nei BDAR, nei EDAV gairėse. Sistemiškai vertinant aptartas nuostatas, disertacijos autoriaus nuomone, duomenų tvarkymas pagal ribų valdymo mechanizmus viešoje vietoje numatančius nacionalinius teisės aktus galėtų patekti tiek į BDAR 6 straipsnio 2 dalies c punkte, tiek į BDAR 6 straipsnio 2 dalies e punkte nurodytą pagrindą. Po kuriuo duomenų tvarkymo pagrindo skėčiu papultų atitinkamas duomenų tvarkymas priklausytų nuo elgesio modelio, kurį nacionaliniu teisės aktu norima išsaugoti arba slopinti. Tais atvejais, kai nacionaliniu teisės aktu būtų slopinami tam tikru elgesio šablonai, valdžios institucijos turėtų pasverti, ar slopinimas būtų proporcingas. Taigi nacionalinių teisės aktų priėmimas vadovaujantis disertacijos autoriaus siūloma ribų valdymo teorija neturėtų prieštarauti BDAR.

4.2.4. Poskyrio išvados

Apibendrinant galima teigti, kad šiuo metu labiausi tikėtini duomenų tvarkymo pagrindai, kuriais vadovautųsi bepiločių orlaivių valdytojai, yra duomenų subjekto sutikimas (BDAR 6 straipsnio 1 dalies a punktas) ir „teisėtas interesas“ (BDAR 6 straipsnio 1 dalies f punktas).

Sutikimo pagrindas (BDAR 6 straipsnio 1 dalies a punktas), nors teoriškai laikomas tinkamu, praktikoje yra sunkiai įgyvendinamas, ypač kai skrydžiai vykdomi viešose vietose. Gauti visų galimai stebimų asmenų sutikimą iš anksto yra beveik neįmanoma, o reikalavimas tai daryti sukurtų nerealius apribojimus tiek fiziniams asmenims, tiek komerciniams operatoriams. Pagal ESTT praktiką „namų ūkio išimtis“ netaikoma duomenų rinkimui viešose erdvėse, tačiau toks požiūris bepiločių orlaivių atveju atrodo per griežtas ir nepritaikytas realioms naudojimo situacijoms. Pramoginiais tikslais skraidinantys fiziniai asmenys dažniausiai nesiekia sistemingai rinkti asmens duomenų, todėl BDAR reikalavimai neturėtų būti taikomi jiems taip pat griežtai, kaip organizacijoms, vykdančioms stebėseną.

Alternatyvus duomenų tvarkymo pagrindas – teisėtas interesas (BDAR 6 straipsnio 1 dalies f punktas) – gali būti tinkamas bepiločių orlaivių naudojimui žurnalistikos, mokslinių tyrimų ar viešojo intereso tikslais. Vis dėlto šis pagrindas yra gana abstraktus ir gali būti interpretuojamas skirtingai, priklausomai nuo aplinkybių. Siekiant aiškumo, būtina užtikrinti proporcingumo principo taikymą – duomenų tvarkymas neturi pažeisti duomenų subjektų teisių labiau, nei būtina siekiant teisėto intereso.

Vienas iš galimų sprendimų – nacionalinis reguliavimas pagal BDAR 6 straipsnio 2 dalį, kuris galėtų aiškiau apibrėžti bepiločių orlaivių naudojimo ribas ir užtikrinti pusiausvyrą tarp privatumo apsaugos ir technologinės plėtros. Nacionalinis teisės aktas galėtų leisti duomenų tvarkymą be sutikimo tam tikromis sąlygomis, pavyzdžiui, jei surinkti duomenys netampa dalimi sistemingos stebėsenos arba jei asmens tapatybę nustatyti nėra lengva. Tokia teisinė sistema leistų aiškiau atskirti, kada BDAR taikomas, o kada fiziniai asmenys ar tam tikros

organizacijos galėtų naudoti bepiločius orlaivius be perteklinių reguliavimo naštų.

4.3. BDAR siūlomos privatumo apsaugos priemonės

Pereinant prie BDAR siūlomų privatumo apsaugos priemonių, kurios siejasi su bepiločiais orlaiviais, aktualu aptarti pagrindinius BDAR bendruosius asmens duomenų tvarkymo reikalavimus, pritaikytosios ir standartizuotosios duomenų apsaugos principus, duomenų pseudonimizavimą ir poveikio duomenų apsaugai vertinimus.

4.3.1. Bendrieji asmens duomenų tvarkymo reikalavimai

Visų pirma, BDAR nenumato atskirų reikalavimų bepiločių orlaivių vykdomai stebėsenai, todėl vertėtų trumpai aptarti bendruosius reikalavimus asmens duomenų tvarkymui, kurių privaloma laikytis pagal BDAR. Asmens duomenų tvarkymas pagal BDAR yra teisėtas, kai laikomasi šių 5 straipsnyje numatytų principų ir iš jų kylančių reikalavimų:

1. *Teisėtumo, sąžiningumo ir skaidrumo principo,* kuris bepiločių orlaivių atveju būtų įgyvendinamas tinkamai informuojant stebimuosius.

2. *Tikslo apribojimo principo,* kuris būtų užtikrinamas, jei skrydžio bepiločiu orlaiviu metu surinkti vaizdo ar garso duomenys būtų tvarkomi tik tais tikslais, dėl kurių jie buvo surinkti.

3. *Duomenų kiekio mažinimo principo,* kuris būtų užtikrinamas, jei skrydžio bepiločiu orlaiviu metu būtų renkami tik tie duomenys, kurie yra būtini nustatytam teisėtam tikslui pasiekti.

4. *Tikslumo principo,* kuris iš esmės reiškia, jog tais atvejais, kai bepiločiu orlaiviu surinkta informacija yra netiksli, būtina užtikrinti, jog ji bus nedelsiant ištrinta ar ištaisyta.

5. *Saugojimo trukmės apribojimo principo,* kuris būtų užtikrintas, jei bepiločiu orlaiviu surinkti duomenys būtų saugomi tiktai tiek, kiek tai būtina atitinkamam teisėtam tikslui pasiekti. Ilgiau archyvuoti bepiločiu orlaiviu surinktą informaciją būtų leidžiama tik viešojo intereso labui, atliekant mokslinius ar istorinius tyrimus, taip pat ir statistiniais tikslais.

6. *Vientisumo ir konfidencialumo principo,* kuris galėtų būti užtikrinamas bepilotį orlaivį apsaugant nuo įsilaužimų, duomenų ryšio perėmimų, apie kuriuos jau kalbėta ankstesniame disertacijos skyriuje[572], taip pat apsaugant surinktus duomenis nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

7. *Duomenų subjektų teisių gerbimo ir jų įgyvendinimo užtikrinimo,* kuris būtų užtikrinamas stebimiems asmenims suteikiant galimybę susipažinti su bepiločiu orlaiviu surinktais duomenimis ir, esant pagrindui, prieštarauti dėl jų tvarkymo.

572 Žr. disertacijos 1.5.4 poskyrį.

8. *Atskaitomybės principo, kuris būtų užtikrinamas,* jeigu bepiločio orlaivio valdytojas laikytųsi BDAR reikalavimų ir gebėtų tai įrodyti[573].

Disertacijos autoriaus vertinimu, šie BDAR įtvirtinti principai abstraktūs, todėl konkrečios informacijos apie tai, kaip turėtų būti įgyvendinama duomenų apsauga bepiločių orlaivių valdytojams nesuteikia. Vis dėlto tai nebūtinai neigiamas dalykas. Kol bepiločių orlaivių technologija toliau vystosi, BDAR principai veikia kaip standartizavimo pagrindas, kuriuo vadovaudamiesi bepiločių orlaivių rinkos dalyviai (projektuotojai, gamintojai ir valdytojai), gali užsiimti kryptinga savireguliacija, rengdami vidines tvarkas.

Tobulėjant bepiločių orlaivių technologijoms ir jų panaudojimo galimybėms vykdyti stebėseną didesniu mastu turėtų atsirasti tarptautinės ir nacionalinės jurisprudencijos, kurioje, tikėtina, ateityje būtų išgryninamos gerosios praktikos bepiločių rinkoje pavyzdžiai. Galiausiai geroji praktika, kurią pripažįsta teismai, galėtų būti pritaikyta ir specifiniam formaliam bepiločių orlaivių reguliavimui, kuris geriausiu atveju būtų paremtas ribų valdymo teorijos pagrindu išgrynintais visuomenės elgesio modeliais, kuriuos valstybės rinktųsi išsaugoti arba slopinti. Disertacijos autoriaus vertinimu, tikėtina, jog toks kelias pernelyg nesuvaržytų bepiločių orlaivių technologijos raidos ir padarytų ateities inovacijas šioje srityje „privatumui jautrias".

4.3.2. Pritaikytoji ir standartizuotoji duomenų apsauga

Gaires bepiločių orlaivių rinkos procesų standartizavimui suteikia BDAR 25 straipsnyje bei preambulės 78 punkte įtvirtintais pritaikytosios duomenų apsaugos (angl. *privacy by design*) ir standartizuotosios duomenų apsaugos (angl. *privacy by default*) principai[574]. Paprastai tariant, pritaikytoji ir standartizuotoji duomenų apsauga reiškia, jog kiekviename bepiločių orlaivių rinkos lygmenyje dalyvaujantys subjektai – nuo projektuotojų iki valdytojų – turėtų stengtis į pačią bepiločių orlaivių technologiją ir vidinius įmonės procesus inkorporuoti privatumo apsaugą. Diskrecija, kokias priemones pasirinkti, priklauso nacionalinėms valdžios institucijoms ir patiems rinkos dalyviams.

Pasak LR valstybinės duomenų apsaugos inspekcijos (toliau – VDAI), sprendžiant, kokios techninės ir organizacinės priemonės turėtų būti taikomos, atsižvelgiama į tokius aspektus kaip techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas, duomenų tvarkymo pobūdį, duomenų tvarkymo aprėptį, duomenų tvarkymo kontekstą, duomenų tvarkymo tikslą, į įvairių tikimybių ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms[575]. Rekomendacijose apie vaizdo duomenų

---

573 BDAR, 5 straipsnis; „Rekomendacija dėl vaizdo duomenų tvarkymo daugiabučiuose ir privačiuose gyvenamuosiuose namuose", VDAI, (2019): 3.

574 Bendrasis asmens duomenų reglamentas, 25 straipsnis, preambulės 78 punktas.

575 „Rekomendacija dėl vaizdo duomenų tvarkymo daugiabučiuose ir privačiuose gyvenamuosiuose namuose", *supra note,* 577: 6.

tvarkymą daugiabučiuose ir privačiuose gyvenamuosiuose namuose VDAI taip pat pateikia keletą konkrečių techninių ir organizacinių priemonių pavyzdžių, kurie galėtų būti išdėstyti vaizdo duomenų apsaugos politikoje ar duomenų tvarkymo taisyklėse, kaip antai:

- Duomenų valdytojui vaizdo stebėjimą vykdant turto saugos tikslais, duomenis pakanka saugoti nuo savaitės iki 1 mėnesio, išskyrus atvejus, kai gaunamas pavojaus signalas arba prašymas iš teisėsaugos institucijų. Tuomet yra pagrindas vaizdo įrašą saugoti ilgiau ir laukti policijos ar teismo institucijų sprendimo.

- Kai vykdoma daugiabučio namo stebėsena, prie duomenų turėtų turėti prieigą tik daugiabučio namo įgaliotas asmuo (pirmininkas) ir (ar) pagal paslaugų sutartį pasamdyti darbuotojai, o ne visi daugiabučio namo gyventojai.

- Prieigą prie vaizdo kamerų būtina apsaugoti unikaliais vartotojų vardais ir slaptažodžiais, kad būtų užtikrinamas duomenų saugumas[576].

Nors šie pavyzdžiai tiesiogiai nesusiję su bepiločių orlaivių naudojimu, bet tai yra puiki iliustracija, kokių techninių ir organizacinių priemonių VDAI galėtų tikėtis iš bepiločių orlaivių rinkos dalyvių.

Disertacijos darbo autoriaus vertinimu, pritaikytosios ir standartizuotosios duomenų apsaugos principai, kaip ir bendrieji asmens duomenų tvarkymo principai, daug aiškumo bepiločių orlaivių rinkos dalyviams nesuteikia, tačiau, kaip jau aptarta, tokiu būdu sudaromos geresnės sąlygos bepiločių technologijos vystymuisi ir kryptingai šios rinkos savireguliacijai.

4.3.3. Pseudonimų suteikimas asmens duomenims, šifravimas ir anonimiškumas

Kaip vieną iš konkrečių priemonių, galinčių apsaugoti privatumą, BDAR numato pseudonimų suteikimą[577], kuris apibrėžiamas kaip „asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti“[578].

Pseudonimų suteikimo asmens duomenims nereikėtų maišyti su anonimiškai tvarkoma informacija, t. y. anonimizavimu. Paprastai tariant, pseudonimų suteikimas yra duomenų apsaugos priemonė, kuria duomenys užšifruojami taip, kad duomenų subjektas negalėtų būti tiesiogiai atpažįstamas, bet duomenis galima sugrąžinti į originalią formą turint šifravimo raktą. O anonimiškai pateikti

576 *Ibid.,* 6–7.
577 BDAR, preambulės 28 punktas.
578 *Ibid.,* 4 straipsnio 5 punktas.

duomenys yra tokia apsaugos priemonė, kai automatiniu būdu asmens duomenys depersonalizuojami taip, kad iš jų neįmanoma asmens identifikuoti naudojant praktinius metodus. Pagrindinis skirtumas yra tas, kad pagal BDAR iš asmens duomenų, kuriems suteiktas pseudonimas, pasinaudojus papildoma informacija galima identifikuoti atitinkamą asmenį, todėl tokie duomenys patenka į šio teisės akto taikymą sritį, o anonimiškai pateikti duomenys jau nebelaikomi asmens duomenimis ir į BDAR taikymo sritį nepatenka[579].

Kartu su pseudonimų suteikimu asmens duomenims BDAR siūlo taikyti ir duomenų šifravimą[580]. Tai iš esmės duomenų saugos metodas, dėl kurio duomenys tampa nesuprantami prieigos teisės neturintiems asmenims. Prie tokių duomenų gali prieiti tik šalys, turinčios prieigą prie dekodavimo mechanizmo ir slapto šifravimo rakto[581]. Šifravimas yra vienas iš techninių būdų, kuriuo duomenims galima suteikiamas pseudonimas[582].

Manytina, jog visos aptartos privatumą saugančios priemonės gali būti pritaikytos bepiločių orlaivių kontekste, todėl vertėtų detaliau aptarti teisines pasekmes, kurias sukelia kiekvienos iš jų naudojimas.

Tokios priemonės, kaip bepiločiu orlaiviu surinktų duomenų šifravimas ir pseudonimų suteikimas asmens duomenims, reikšmingai sumažina subjektų, kurie gali tuos duomenis panaudoti, skaičių. Pvz., įmonė X turi bepiločių orlaivių spiečių, kuriuo fiksuotą vaizdo medžiagą laiko debesijos saugykloje, priklausančioje įmonei Y. Perkeldama vaizdo įrašus į debesijos saugyklą, įmonė Y kliento duomenis automatiškai šifruoja raktu, kurį turi tiktai įmonė X. Šiame pavyzdyje įmonė X – duomenų valdytojas, o įmonė Y – duomenų tvarkytojas. Formaliai duomenų tvarkytojas (įmonė Y) vis dar turi prieigą prie duomenų, kuriuos jos serveriuose išsaugojo duomenų valdytojas (įmonė X), tačiau tie duomenys, t. y. vaizdo įrašai, neturi jokios prasmės, nes duomenų tvarkytojas (įmonė Y) vaizdo įrašų atidaryti jokia vaizdo rodymo programa negali, kol šie nėra dekoduoti tiktai duomenų valdytojui (įmonei X) žinomu prieigos raktu. Tokių tvarkytojų kaip įmonė Y šių laikų internetu sujungtame pasaulyje gali būti daugybė, tačiau prieigą prie dekoduotų duomenų turės tik vienas subjektas – duomenų valdytojas.

Be abejo, egzistuoja teorinė tikimybė, jog įmonė Y sužinos įmonei X priklausantį raktą iš, pvz., įmonės X darbuotojų ar naudodama neteisėtus dešifravimo metodus. Paprasčiausi ir labiausiai paplitę programišių naudojami dešifravimo būdai yra *išsami raktų paieška* (angl. *exhaustive key search*) arba žiaurios jėgos atakos (angl. *brute-force attacks*), kurių veikimo principas yra

579 BDAR, preambulės 26 punktas.

580 BDAR 6 straipsnio 4 dalies e punkte siūloma taikyti pseudonimizavimą ARBA šifravimą, 32 straipsnio 1 dalies a punkte siūloma pseudonimizavimą IR šifravimą. Vis dėlto, disertacijos darbo autoriaus vertinimu, pseudonimizavimas veiktų kaip privatumą apsauganti technologija geriausiai, jeigu duomenys papildomai būtų dar ir šifruojami.

581 Giuseppe D'Acquisto ir kt., *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics,* 2015, https://doi.org/10.2824/641480.

582 „Opinion 05/2014 on Anonymisation Techniques", Article 29 data protection working party, 0829/14/EN, WP216.

išbandyti visus įmanomus raktus ir galiausiai atspėti teisingąjį[583]. Todėl BDAR duomenis, kuriems suteikti pseudonimai ar yra šifruoti, priskiria prie asmens duomenų.

Tačiau nekyla abejonių, jog šifruoti duomenys būtų labiau apsaugoti, negu nešifruoti, todėl šiais laikais jau plačiai taikoma privatumą sauganti technologija, kurią vertėtų taikyti ir duomenims, renkamiems bepiločiais orlaiviais.

Kiekvieno duomenų rinkinio šifravimas turėtų apsunkinti darbą masinę stebėseną vykdančioms valdžios institucijoms, kurios norėdamos prieiti prie šifruotos informacijos, turėtų pirmiausia kažkokiu būdu gauti duomenų valdytojui priklausantį šifravimo raktą, kuris gali būti sunkiai pasiekiamas, jeigu laikomas atskirai nuo duomenų rinkinio (pvz., įmonės X direktorius jį gali būti užsirašęs ant popieriaus lapo ir pasidėjęs į fizinį seifą, į kurį slapta įsilaužti gali būti ypač sudėtinga). Tad ir tokiu atveju duomenų šifravimas suteiktų didesnę privatumo apsaugą nei nešifravimas. Vis dėlto turėtų būti užtikrinama, kad šifravimo technologijoje nebūtų palikta atsitiktinių klaidų ar sisteminių „galinių durų", kurios tokią prieigą valdžios institucijoms vis tiek suteiktų[584].

Diskutuojant apie duomenų anonimiškumą bepiločių orlaivių atveju, teoriškai tai turėtų būti dar geresnė privatumo apsaugos priemonė negu šifravimas ar pseudonimų suteikimas, nes surinkti asmens duomenys būtų negrįžtamai depersonalizuojami, todėl būtų išvengiama *identifikavimo, saugumo neužtikrinimo* ir *atidengimo* privatumo pažeidimų[585]. Vis dėlto yra tam tikrų niuansų, susijusių su šios privatumą saugančios priemonės taikymu.

Pirma, anonimizavimas veiktų visa apimtimi tik tada, jeigu duomenys būtų depersonalizuojami realiu laiku pačioje skraidyklėje, bet šiuo metu tokia technologinė inovacija, kuri būtų pritaikyta būtent bepiločių orlaivių technologijai, neegzistuoja. Tad reikia preziumuoti, kad bepiločiu orlaiviu surinkti duomenys pirmiausia atsidurs kokioje nors duomenų laikmenoje ar nuotoliniame serveryje. Šiame etape dalyvaus bepiločiu orlaiviu surinktų duomenų valdytojas, o jei duomenys laikomi serveryje, tai ir duomenų tvarkytojas, kuriems bus taikomi BDAR reikalavimai. Tuomet duomenys turės būti „paleidžiami" per specialią programinę įrangą, kuri juos turėtų grąžinti jau depersonalizuotus. Kol duomenys būtų anonimizuojami, jie, esant dabartinėms technologinėms galimybėms, turėtų įveikti kelis etapus, kuriuose dalyvautų tiek duomenų valdytojas, tiek duomenų tvarkytojai pagal BDAR tvarką.

DG29 taip pat laikosi prielaidos, kad taikant anonimizavimą duomenys pirmiausia būtų surenkami ir talpinami laikantis teisės aktų nustatančių reikalavimus duomenų saugojimui. Taip pat pastebi, jog, pasibaigus numatytam saugojimo

583 Bart van der Sloot, Dennis Broeders ir Erik Schrijvers, *Exploring the boundaries of Big Data* (Amsterdam: University Press Amsterdam, 2016).

584 Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): 172.

585 Žr. disertacijos 1 skyrių.

terminui, duomenų valdytojas juos galėtų anonimizuoti ir toliau laikyti savo duomenų bazėse „tolesnio apdorojimo“ tikslais. Aišku, DG29 nuomone, vertinant, ar gali būti tęsiamas tolesnis apdorojimas, pritaikyti vadinamąjį „suderinamumo testą“, kuris nustatytų tolesnio saugojimo būtinumą ir pasekmes duomenų subjektams[586].

Nors teoriškai iš tokių anonimiškų duomenų neturėtų būti įmanoma nustatyti subjektų tapatybių, praktikoje buvo atvejų, kai duomenis pavyko deanonimizuoti, o juose esančius asmenis reidentifikuoti[587]. Taip pat yra manančių, jog dabartiniai sprendimai, taikomi anonimizuojant duomenis, dar nepakankamai išvystyti, kad galėtų būti naudojami plačiai[588]. Nereikėtų pernelyg nuogąstauti, juk technologijos nuolat vystosi, tad situacija ateityje galima iš esmės keistis. Tačiau net ir tikintis, kad technologijos jau dabar leidžia ar ateityje leis patikimą individų depersonalizavimą bepiločių orlaivių surinktuose duomenyse, didelę galią rinkoje turintys privatūs subjektai, disponuojantys didžiausiais duomenų rinkiniais, gali nesivarginti anonimizuoti iki tokio lygio, kad negalėtų būti identifikuojami ne tik konkretūs asmenys, bet asmenų grupių ar didelių minių elgesio modeliai. Kitaip tariant, jie gali duomenis anonimizuoti tik tiek, kiek būtina formaliai užtikrinti teisės aktų reikalavimus, tačiau iš disponuojamos anonimizuotos informacijos vis tiek daryti reikšmingas įžvalgas apie visuomenės elgesio šablonus.

Pvz., įmonė surinktuose duomenyse gali užmaskuoti žmonių veidus, bet palikti matomą jų aprangą, kūno judesius, supančią aplinką. Iš tokių duomenų įmonė galėtų nustatyti žmonių skaičių, jų lytį, galimai netgi amžių. Tam tikrais atvejais agreguodama surinktą informaciją su viešai prieinama informacija, pvz., socialiniuose tinkluose paskelbtomis nuotraukomis, tokia įmonė netgi galėtų reidentifikuoti daugelį asmenų iš jų aprangos ar kūno judesių. Iš tokios informacijos būtų galima nustatyti netgi žmonių judėjimo srautus, atskirų visuomenės grupių elgesio šablonus ir pan. Panaši situacija yra nutikusi realiai[589]. „Privatumo praradimo“ grėsmes, kylančias taikant duomenų anonimizavimą, įžvelgia ir DG29[590].

Kadangi anonimiška informacija nepatenka į BDAR taikymo sritį, ji ilgainiui gali įgauti ne privatumą saugančios technologijos, o BDAR reikalavimų padedančios išvengti technologijos reputaciją. Tačiau kadangi įmonės stengtųsi formalią atitiktį užtikrinti, aptartas privatumui žalingas praktikas aptikti būtų

---

586 „Opinion 05/2014 on Anonymisation Techniques“, *supra note,* 586: 7.

587 Žr. Paul Ohm, „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“, *UCLA Law Review* 57, 6 (2009): 1701–1778.

588 Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR“, 2019 IEEE International Congress on Big Data (BigDataCongress) *(2019 IEEE International Congress* on Big Data (BigData Congress), Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.

589 Michael Barbaro ir Tom Zeller Jr, „A Face Is Exposed for AOL Searcher No. 4417749“, *The New York Times,* 2006 m. rugpjūčio 9 d., https://www.nytimes.com/2006/08/09/technology/09aol.html.

590 „Opinion 05/2014 on Anonymisation Techniques“, *supra note,* 586: 11.

įmanoma tik per korporatyvinio šnipinėjimo atvejus (angl. *corporate espionage*) ar informacijos nutekėjimo skandalus (angl. *whistle-blower scandals*).

DG29 pastebi, jog veiksmingas duomenų anonimiškumas neleistų nustatyti atskiro individo duomenų rinkinyje, taip pat susieti dviejų įrašų tame pačiame duomenų rinkinyje (arba tarp dviejų atskirų duomenų rinkinių) ir taip išvesti naują informaciją. Todėl vien pašalinti tiesiogiai identifikuojančius elementus nepakanka, kad būtų užtikrinta, jog duomenų subjekto tapatybės nebus įmanoma nustatyti. Dažnai reikės imtis papildomų priemonių, kad būtų išvengta tapatybės nustatymo, atsižvelgiant į duomenų tvarkymo, kuriam skirti anoniminiai duomenys, kontekstą ir tikslus. Vis dėlto daugelis dabar prieinamų anonimizavimo technologijų turi imanentinių trūkumų, dėl kurių visiškai duomenis anonimizuoti šiuo metu neįmanoma[592]. Taip pat tikėtis, jog didelę galią rinkoje turintys subjektai geranoriškai laikysis tokios gerosios praktikos, yra trumparegiška.

Vietoj to, disertacijos autoriaus nuomone, teisės aktais verčiau reikėtų įtvirtinti konkretų anonimiškų duomenų saugojimo terminą, kad jie negalėtų būti laikomi neribotai. Tam tikra apimtimi tai įgyvendina elektroninių ryšių stebėseną reguliuojantys teisės aktai, numatantys ribotą duomenų saugojimo terminą, kuomet nesvarbu, ar juose duomenys anonimiški, ar ne[593], bet į jų taikymo sritį bepiločiais orlaiviais renkama informacija nepatektų.

Taigi, manytina, jog šifravimas ir pseudonimų suteikimas bepiločių orlaivių kontekste turėtų būti veiksmingos duomenų apsaugos priemonės, nes reikšmingai sumažintų asmenų, kurie gali prieiti prie surinktų duomenų, skaičių. Šios technologijos gerai išvystytos ir jau taikomos praktiškai, todėl turėtų prisidėti prie privatumo apsaugos, vykdant bepiločiais orlaiviais skrydžius, jau šiuo metu. Anonimizavimas teoriškai turėtų būti puiki privatumą apsauganti technologija, kuri bepiločių orlaivių atveju veiktų geriausiai, jeigu asmens duomenys būtų depersonalizuojami realiu laiku pačioje skraidyklėje, o iki tol galima pasikliauti šifravimo ir pseudonimų suteikimo sprendimais. Ateityje pradėjus anonimizavimą taikyti didesniu mastu, tam, kad jis pasiteisintų, būtina technologiškai užtikrinti, jog duomenų nebebūtų įmanoma deanonimizuoti, o teisės aktais būtų apribotas tokių duomenų saugojimo terminas.

4.3.4. Poveikio duomenų apsaugai vertinimai

Dar viena BDAR numatyta privatumo apsaugos priemonė, kuri aktuali naudojant bepiločius orlaivius, – tai reikalavimas atlikti poveikio duomenų apsaugai vertinimą (toliau – PDAV). PDAV turėtų padėti iš anksto identifikuoti ir išanalizuoti grėsmes, kurios gali kilti individams dėl atitinkamos technologijos ar

591 *Ibid.,* 9.
592 *Ibid.,* 24.
593 Žr. LR elektroninių ryšių įstatymas, *supra note,* 181: 78 straipsnio 3 dalis.
594 BDAR, 35 straipsnis.

proceso, tarp jų ir bepiločių orlaivių, naudojimo. Pagal BDAR 35 straipsnį tokia priemonė taikoma tais atvejais, kai dėl duomenų tvarkymo žmogaus teisėms, tarp jų ir privatumui, gali kilti didelis pavojus[594]. Dideliu pavojumi BDAR laikomi atvejai:

1. Kai duomenys automatiniu būdu sistemingai ir išsamiai vertinami, siekiant išanalizuoti fizinių asmenų elgesį, įskaitant profiliavimą, ir juo remiantis priimami sprendimai, darantys teisinį ar kitą didelį poveikį fiziniam asmeniui.

2. Kai jautrūs duomenys arba duomenys apie apkaltinamuosius nuosprendžius bei nusikalstamas veikas tvarkomi dideliu mastu.

3. Kai atliekamas sistemingas viešos vietos stebėjimas dideliu mastu[595].

Lietuvos valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymu yra patvirtintas ir papildomų atvejų sąrašas, kada PDAV būtų privalomas. Atvejai, kurie aktualūs vykdant bepiločių orlaivių stebėseną, būtų šie:

1. Mokslinių ar istorinių tyrimų tikslais specialių kategorijų asmens duomenys[596] tvarkomi be duomenų subjekto sutikimo.

2. Mokslinių ar istorinių tyrimų tikslais asmens duomenys tvarkomi susiejant ar derinant duomenų rinkinius.

3. Asmens duomenys tvarkomi dideliu mastu ir jie buvo gauti ne iš duomenų subjekto, kai neįmanoma arba labai sudėtinga duomenų subjektui pateikti privalomą informaciją pagal BDAR 14 straipsnį[597].

4. Kai stebėsenos ar kontrolės tikslais renkami biometriniai duomenys.

5. Kai stebėsenos ar kontrolės tikslais tvarkomi darbuotojų asmens duomenys.

---

595 *Ibid.,* 35 straipsnio 3 dalis.

596 Specialių kategorijų asmens duomenys – tai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose; genetiniai duomenys, biometriniai duomenys, pagal kuriuos galima konkrečiai nustatyti fizinio asmens tapatybę; sveikatos duomenys; duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, VDAI, 3 versija (2020): 5.

597 BDAR 14 straipsnis numato informaciją, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto:
1. Kai asmens duomenys yra gauti ne iš duomenų subjekto, duomenų valdytojas pateikia duomenų subjektui šią informaciją:
a) duomenų valdytojo ir duomenų valdytojo atstovo, jei taikoma, tapatybę ir kontaktinius duomenis;
b) duomenų apsaugos pareigūno, jei taikoma, kontaktinius duomenis;
c) duomenų tvarkymo tikslus, kuriais ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą;
d) atitinkamų asmens duomenų kategorijas;
e) jei jos yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas;
f) kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti gavėjui trečiojoje valstybėje arba tarptautinei organizacijai ir Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, o 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti.

6. Kai vaizdo stebėjimas vykdomas patalpose ar teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais.

7. Kai vaizdo stebėjimas vykdomas kartu su garso įrašymu.

8. Kai asmens duomenys tvarkomi naudojant inovatyvias technologijas.

9. Kai tvarkomi pažeidžiamų duomenų subjektų[598] duomenys, taip pat kai rinkodaros tikslais tvarkomi vaikų duomenys[599].

Reikėtų atkreipti dėmesį, jog tiek BDAR, tiek VDAI direktoriaus įsakymu patvirtinti atvejų sąrašai, kada PDAV yra privalomas, nėra baigtiniai, kiekvienu atveju duomenų valdytojams turint įtarimą, jog gali kilti didelis pavojus žmogaus teisėms, rekomenduojama jį atlikti[600]. Pasak DG29, PDAV nėra vienkartinis veiksmas, pasikeitus aplinkybėms turėtų būti atliekamas iš naujo[601].

BDAR įtvirtintas PDAV procesas jau detalizuotas Lietuvoje VDAI gairėse, kuriose

---

2. Be 1 dalyje nurodytos informacijos, duomenų valdytojas pateikia duomenų subjektui toliau nurodytą papildomą informaciją, būtiną tvarkymo sąžiningumui ir skaidrumui duomenų subjekto atžvilgiu užtikrinti:
a) asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
b) kai duomenų tvarkymas atliekamas pagal 6 straipsnio 1 dalies f punktą, teisėtus duomenų valdytojo arba trečiosios šalies interesus;
c) teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, ir teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į duomenų perkeliamumą;
d) kai duomenų tvarkymas grindžiamas 6 straipsnio 1 dalies a punktu arba 9 straipsnio 2 dalies a punktu, teisę bet kuriuo metu atšaukti sutikimą, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui;
e) teisę pateikti skundą priežiūros institucijai;
f) koks yra asmens duomenų kilmės šaltinis, ir, jei taikoma, ar duomenys gauti iš viešai prieinamų šaltinių;
g) tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui.

598 Pažeidžiamiems duomenų subjektams gali priklausyti vaikai (juos galima laikyti negalinčiais sąmoningai ir apgalvotai prieštarauti savo duomenų tvarkymui arba sutikti su duomenų tvarkymu), darbuotojai, pažeidžiamesni gyventojų, kuriems reikalinga speciali apsauga, segmentai (psichiškai nesveiki asmenys, prieglobsčio prašytojai arba vyresnio amžiaus asmenys, pacientai ir pan.), ir visais atvejais, kai galima nustatyti nelygiaverčius duomenų subjekto ir duomenų valdytojo santykius. „Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų", 29 straipsnio duomenų apsaugos grupė, WP 248, 1-oji peržiūrėta versija, 17/LT (2017).

599 „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo", Valstybinės duomenų apsaugos inspekcijos direktorius, 1T-35 (1.12.E), TAR, 2019-03-14, Nr. 4104.

600 Tokią išvadą galima daryti sistemiškai vertinant BDAR preambulės 1–4, 10 punktus, 1 straipsnio 1 ir 2 dalį, taip pat Valstybinės duomenų apsaugos inspekcijos direktoriaus aptvirtinto Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo preambulę.

601 „Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų", *supra note,* 602: 16.

nurodoma, jog PDAV susideda iš keturių pagrindinių žingsnių (nors jį galima skaidyti ir į daugiau žingsnių, kuriuos gali nusistatyti pati organizacija)[602].

Pirmiausia stebėseną bepiločiais orlaiviais vykdanti organizacija turėtų nustatyti duomenų tvarkymo operacijos pobūdį ir jos kontekstą. Šiame etape VDAI siūlo įvertinti: (i) kokios yra organizacijos asmens duomenų tvarkymo operacijos, (ii) kokios kategorijos asmens duomenys yra tvarkomi, (iii) koks tvarkymo tikslas, (iv) kokios priemonės naudojamos tvarkyti asmens duomenis, (v) ar vykdomas asmens duomenų tvarkymas, (vi) kokios yra duomenų subjektų kategorijos, (vii) kas yra duomenų gavėjai[603].

Toliau pagal pirmame žingsnyje atliktą analizę turėtų būti įvertinamas rizikos duomenų apsaugai lygis. Pasak VDAI, *žemas* rizikos lygis reiškia, jog fizinis asmuo gali sugaišti laiką iš naujo suvesdamas informaciją, susierzinti, patirti nepasitenkinimą ir pan., t. y. susidurti su tam tikrais nepatogumais. *Vidutinio* rizikos lygio, pvz., galėtų būti papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir pan., dėl kurių individas patirtų didelių nepatogumų, kuriuos nepaisant sunkumų galėtų įveikti. *Aukšto* rizikos lygio, pvz., būtų lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas, negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan., t. y. tokios pasekmės, kurios individui sukeltų rimtų sunkumų arba lemtų didelius ar negrįžtamus pokyčius[604]. Siekiant tinkamai nustatyti galimą duomenų tvarkymo poveikį, duomenų valdytojams siūloma atskirai įvertinti poveikį įvykus duomenų konfidencialumo, vientisumo ir prieinamumo praradimui naudojantis gairėse pateikta lentele[605].

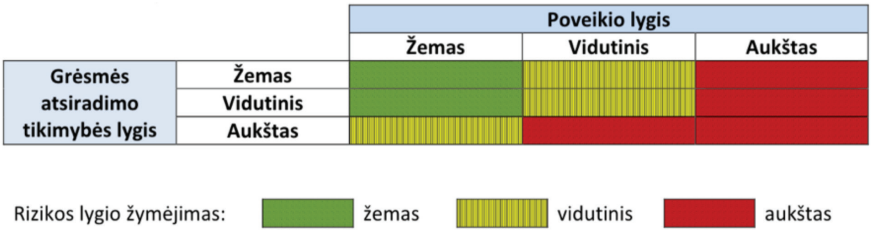
Trečiame etape duomenis valdančiai ar tvarkančiai organizacijai reikia, naudojantis VDAI pateikta lentele, nustatyti išorės arba vidaus grėsmes, susijusias su duomenų tvarkymo aplinka. Kitaip tariant, vertinamos duomenų nutekėjimo rizikos dėl nepakankamo saugumo užtikrinimo, neaiškių instrukcijų ir procedūrų kaip su asmens duomenimis reikia elgtis, dėl per didelio darbuotojų, tvarkančių duomenis, skaičiaus, potencialių užpuolikų ir pan.[606]

Paskutinis etapas skirtas vertinimo rezultatams suvesti į lentelę (žr. 8 lentelę[607]) ir rizikos lygiui įvertinti pagal duomenų tvarkymo operacijos poveikį bei atitinkamos grėsmės atsiradimo tikimybę.

---

602 „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“, *supra note,* 603.
603 „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, *supra note,* 600: 4.
604 *Ibid.*
605 *Ibid.,* 5.
606 *Ibid.,* 5–7.
607 *Ibid.,* 8.

8 lentelė. *PDAV rizikos lygio įvertinimas*



Atlikus PDAV pagal rizikos, kylančios duomenų apsaugai, lygį VDAI rekomenduoja taikyti priemones, kurios papildomai suskirstytos į dvi kategorijas (organizacines ir technines). Keli organizacinių priemonių pavyzdžiai, *inter alia,* yra:

- Organizacijos asmens duomenų politikos patvirtinimas.
- Duomenų valdytojai turėtų pasitvirtinti vidines gaires ir procedūras, kurios detalizuotų asmens duomenų tvarkymo procesus.
- Organizacijos turėtų patvirtinti vidines saugumo incidentų likvidavimo tvarkas.
- Organizacijos turi užtikrinti duomenų saugos procedūrų tęstinumą, pvz., paskirdamos duomenų apsaugos pareigūną, parengdamos tęstinumo planą.
- Organizacijos turi rengti vidinius mokymus duomenų saugos tema[608].

Tarp techninių priemonių VDAI gairėse, *inter alia,* minimos šios:

- Organizacija turėtų turėti Prieigų kontrolės sistemą, per kurią galėtų kurti, tvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.
- Prisijungimai prie duomenų tvarkymo sistemų turėtų būti saugūs (pvz., vengiama vienodų, lengvų slaptažodžių, naudojamas dviejų veiksnių autentifikavimas ir pan.).
- Turi būti vedami techniniai žurnalai, kuriuose būtų matyti darbuotojų prieigų prie asmens duomenų sistemų laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai).
- Duomenų bazės, kuriose kaupiami asmens duomenys, turėtų būti apsaugotos šifravimo sprendimais.
- Organizacijos turėtų užtikrinti darbo vietų apsaugą nuo neleistinos prieigos (pvz., turėtų būtų neleidžiama duomenis iš darbinio kompiuterio perkelti į USB, DVD laikmenas, turėtų būti įdiegtos anti-virusinės programos, standusis diskas turėtų būti šifruotas ir pan.).

608 *Ibid.,* 9–18.

- Turi būti užtikrinama tinklo ir komunikacijos sauga (pvz., belaidė prieiga turėtų būti apsaugota šifravimo mechanizmais, turi būti naudojamos ugniasienės, turi būti vykdoma MAC adresų prieigos kontrolė ir pan.).
- Atsarginės kopijos turėtų būti šifruojamos, reguliariai testuojamos.
- Prieigai prie mobiliųjų, nešiojamųjų įrenginių turėtų būti naudojamas dviejų veiksnių autentifikavimas[609].

Disertacijos autoriaus vertinimu, PDAV iš esmės yra viena iš privatumą pagal ribų valdymo teoriją saugančių priemonių. Ribų valdymo teorija, kaip aptarta ankstesniuose skyriuose, orientuojasi į elgesio modelių, kuriuos visuomenė nori išsaugoti ar keisti, reguliavimą. PDAV yra puiki privatumą sauganti priemonė ne tik bepiločių orlaivių, bet ir daugelio kitų naujųjų technologijų kontekste. Bepiločių orlaivių naudojimo atveju ji gali būti suvokiama kaip išankstinio perspėjimo apie galimas privatumo grėsmes sistema, kuria visi duomenų tvarkymo procese dalyvaujantys rinkos žaidėjai (bepiločių orlaivių projektuotojai, gamintojai ir valdytojai) gali sistemiškai įsivertinti potencialius tam tikro proceso trūkumus. Įmonės, prieš pradėdamos naudoti bepiločius orlaivius tam tikrame procese, gali konkrečiai pamatyti, kokias rizikas kelia atitinkamas veiklos modelis, jų priežastis, todėl gali įvertinti būdus, kuriais duomenų saugos režimas gali būti įgyvendinamas organizacijos viduje. Taip pat PDAV leidžia nustatyti tinkamiausią sprendimų priėmimą pradiniuose verslo projektų vykdymo etapuose, taip galima išvengti didelių nuostolių netikėtai netekėjus duomenims tolesniuose vystymo etapuose.

PDAV skatina rinkos savireguliaciją, bepiločių orlaivių rinkos žaidėjų švietimą privatumo tema, o tai naudojant bepiločius orlaivius labai svarbus ir, tikėtina, yra veiksmingas būdas iniciatyviu, o ne reaktyviu būdu apsaugoti privatumą nuo pradinių technologijos vystymosi etapų.

4.4. BDAR vertinimas bepiločių orlaivių ir privatumo kontekste

Kaip matyti iš atliktos analizės, bepiločiai orlaiviai į BDAR reguliavimo sritį patenka, nes yra įrankis, kuriuo įmanoma rinkti duomenis. Vis dėlto BDAR skrydžiams, vykdomiems bepiločiais orlaiviais, būtų taikomas ne visada. Pvz., griežtų BDAR reikalavimų nereikėtų laikytis, jeigu iš surinktos vaizdo medžiagos fizinių asmenų neįmanoma identifikuoti arba jeigu surinkti duomenys būtų iš karto anonimizuojami.

Atlikta analizė taip pat parodė, jog bepiločiais orlaiviais duomenis galima rinkti vadovaujantis BDAR 6 straipsnyje nurodytais pagrindais. Tarp jų labiausiai tikėtinas – duomenų subjekto sutikimas. Jį sunkiausia būtų gauti vidutiniams vartotojams, vykdantiems skrydžius viešoje vietoje, bei subjektams, vykdantiems

609 „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, *supra note,* 600: 19–32.

plataus masto stebėseną – pastarieji turėtų remtis kitais teisėtais duomenų rinkimo pagrindais. Įdomu tai, kad pagal ESTT praktiką, suformuotą stacionarių CCTV kamerų kontekste, net ir paprasti vartotojai, vykdydami skrydžius viešoje vietoje pramoginiais tikslais, formaliai turėtų laikytis BDAR reikalavimų. Vis dėlto šios praktikos taikymas vidutiniams naudotojams, vykdantiems skrydžius asmeniniais tikslais, tikriausiai būtų neproporcingas.

Kitas tikėtinas duomenų rinkimo bepiločiais orlaiviais pagrindas yra „teisėtas interesas". Disertacijos autorius analizavo, ar abstrakti šį pagrindą reglamentuojančio BDAR 6 straipsnio 1 dalies f punkto formuluotė nesukuria prielaidų piktnaudžiauti didelę galią rinkoje turintiems subjektams. Vis dėlto prieita prie išvados, jog teismai tikriausiai nebūtų linkę šios nuostatos aiškinti taip plečiamai, kad tuo galėtų piktnaudžiauti didžiųjų duomenų valdytojai.

Vertinant BDAR siūlomas privatumo apsaugos priemones, labiausiai pastebimą naudą privatumo apsaugai suteikia šifravimo technologiniai sprendimai ir poveikio duomenų apsaugai vertinimai. Tačiau abstraktesnės BDAR nuostatos, kurios numato bendruosius asmens duomenų tvarkymo reikalavimus, pritaikytąją ir standartizuotąją duomenų apsaugą, manytina, taip pat reikšmingai prisideda prie privatumo apsaugos, nes veikia kaip standartizavimo šaltinis, kuriuo vadovaudamiesi bepiločių orlaivių rinkos dalyviai (projektuotojai, gamintojai ir valdytojai), kurdami savo vidines tvarkas, gali užsiimti kryptinga savireguliacija.

Analizėje apie šifravimo sprendimus buvo aptarti ir anonimizuoti duomenys, kurie į BDAR taikymo sritį neįeina. Vis dėlto, kaip matyti iš atlikto tyrimo, pasitaikė atvejų, kada duomenys buvo deanonimizuoti, o juose esantys žmonės reidentifikuoti, iš jų buvo įmanoma atpažinti žmonių elgesio šablonus, tačiau šiuo metu teisės aktai ribojimų anonimizuotų duomenų saugojimo trukmei nenumato. Disertacijos autoriaus vertinimu, vertėtų teisės aktais įtvirtinti net ir anonimizuotų duomenų saugojimo terminą, kad privatumui žalingų scenarijų tikimybė būtų kuo mažesnė.

Apibendrinant galima teigti, kad BDAR yra gana abstraktaus pobūdžio privatumo apsaugą reguliuojantis teisės aktas, kuris daugelį reglamento įgyvendinimo aspektų palieka spręsti EDAV, rinkos veikėjams ir nacionalinėms duomenų apsaugos institucijoms. Vis dėlto vienas BDAR aspektas labai griežtai ir išsamiai reglamentuotas – tai reikalavimai duomenų subjekto sutikimui, kuris, kaip parodė atlikta analizė, bepiločių orlaivių kontekste nėra nei patogi, nei veiksminga privatumo apsaugos priemonė. Sutikimas, disertacijos autoriaus vertinimu, yra pagrindinis ES duomenų apsaugos režimo ramstis. Tačiau nors BDAR numato konkrečių privatumo apsaugos priemonių, tokių kaip šifravimo technologiniai sprendimai, poveikio duomenų apsaugai vertinimai bei pritaikytosios ir standartizuotosios duomenų apsaugos doktrinos, ši privatumo apsauga, paremta *savarankiško privatumo valdymo* paradigma, nebūtų veiksminga bepiločių orlaivių naudojimo kontekste, nes gauti sutikimą, leidžiantį rinkti duomenis bepiločiais orlaiviais, būtų ypač sunku. Daugiau apie savarankiško privatumo valdymo paradigmos trūkumus ir galimas išeitis bepiločių orlaivių kontekste bus padiskutuojama kitame

poskyryje.

4.5. Sutikimu paremtos privatumo apsaugos sistemos trūkumai

Kaip parodė atlikta analizė, tiek ES duomenų apsaugos teisės aktai, tiek specialusis bepiločių orlaivių reguliavimas remiasi nuo XX a. aštunto dešimtmečio iš esmės nepakitusia *savarankiško privatumo valdymo* (angl. *privacy self-management*) paradigma[610]. Pagal ją privatumo apsaugos pagrindas yra savarankiškas vartotojo sprendimų priėmimas, kiek savo privataus gyvenimo jis nori atskleisti trečiajam asmeniui mainais į produktus ar paslaugas – tai asmuo įgyvendina per sutikimą. Vis dėlto dauguma tyrėjų atkreipė dėmesį į šios paradigmos trūkumus. Diskusijas kelia tai, jog daugelis vartotojų teigia privatumą labai branginantys, bet jų elgesys išreiškia kardinaliai priešingą požiūrį. Šį reiškinį mokslininkai vadina privatumo paradoksu (angl. *privacy paradox*)[611].

Galima teigti, jog šis atotrūkis egzistuoja dėl šešių pagrindinių priežasčių. *Pirma,* asmenys sutikdami su duomenų tvarkymu nesupranta realių savo pasirinkimo pasekmių. Vienas paaiškinimas gali būti, kad privatumo pranešimai dažniausiai būna ilgi ir sunkiai suprantami. BDAR šią problemą bandoma spręsti taikant skaidrumo principą, numatantį, kad informacija turi būti pateikta glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba[612]. Kaip vieną iš šio principo įgyvendinimo būdų DG29 siūlo, pvz., informaciją pateikti audiovizualiniais metodais[613]. Vis dėlto, nepaisant daugelio bandymų sutrumpinti ar vaizdo priemonėmis padaryti duomenų tvarkymo pranešimus suprantamesnius, anksčiau praktikoje taikytos tokios priemonės nepasiteisino[614]. Su tuo susijusi problema yra ta, kad kuo pranešimai tvarkyti duomenis trumpesni ir paprastesni, tuo sunkiau vartotojus informuoti apie pasekmes, kurias gali sukelti jų pasirinkimas duoti sutikimą, t. y. kuriant tekstus dėl duomenų tvarkymo dažnai reikia ieškoti kompromiso, kaip pateikti informaciją – prasmingai ar trumpai

610 Žr. Solove, „Introduction: Privacy self-management and the consent dilemma“, *supra note,* 36: 1880. („Savarankiško privatumo valdymo“ paradigma yra kilusi iš 1973 m. JAV paskelbtų „Sąžiningos informacijos praktikos principų“ [angl. *Fair Information Practice Principles*], kurių fragmentai 1980 m. buvo perkelti į EBPO privatumo gaires).

611 Žr. Ryan Hagemann, „Consumer Privacy in an Age of Commercial Unmanned Aircraft Systems“, *Independent Review* 23, 1 (2018): 9–22; Benjamin Wittes ir Emma Kohse, *The privacy paradox II: Measuring the privacy benefits of privacy threats* (Center for Technology Innovation at Brookings, 2017); Spyros Kokolakis, „Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon“, *Computers & security* 64 (2017): 122–34.

612 BDAR, 12 straipsnio 1 dalis.

613 „Guidelines on transparency under Regulation 2016/679“, Article 29 data protection working party, 17/EN, WP260 (2018): 9.

614 Ryan Calo, „Against Notice Skepticism in Privacy (and Elsewhere)“, *Notre Dame Law Review* 87 (2011): 1023; Solove, „Introduction: Privacy self-management and the consent dilemma“, *supra note,* 36: 1885.

(paprastai)[615]. Pvz., jeigu duomenys tvarkomi naudojant sudėtingus, save mokančius algoritmus (angl. *self-learning algorithms*), tuomet paaiškinti, kaip bus atliekamas duomenų tvarkymas gali būti apskritai neįmanoma žmonių kalba[616].

Antra, socialinių mokslų tyrimai atskleidžia, jog žmonėms sunku pritaikyti savo žinias sudėtingose su privatumu susijusiose situacijose, kas iškreipia ir sprendimų priėmimą[617]. Įgimtas *ribotas racionalumas* (angl. *bounded rationality*)[618] riboja žmonių gebėjimą įgyti, įsiminti ir apdoroti visą svarbią informaciją, tai verčia individus priimant sprendimus pasikliauti supaprastintais psichikos modeliais, apytikslėmis strategijomis ir euristika[619]. Tinkamą rizikos įvertinimą iškreipia ir *prieinamumo euristika* (angl. *availability heuristic*), kuri reiškia, jog žmonės žinomus pavojus vertina kaip rizikingesnius nei nežinomus[620]. Taip pat paradoksalu, jog kontrolės jausmas, kurį žmonėms suteikia visai nedidelės privatumo kontrolės priemonės (pvz., reikalavimas duoti sutikimą), nesvarbu ar ta kontrolė tikra, ar iliuzinė, skatina juos atskleisti daugiau jautrių asmens duomenų didesnei auditorijai[621]. Kitaip tariant, taikant daugiau privatumo apsaugos priemonių (bet nebūtinai veiksmingų) realiai didinamas atskleidžiamų asmens duomenų kiekis. Remiantis elgsenos tyrimais, taip pat galima teigti, jog žmonių priimami sprendimai labai dažnai būna neracionalūs[622].

Trečia, žmonės norėdami naudotis naujausiomis technologijomis ar paslaugomis internete privalo vadovautis produktų ar paslaugų teikėjų „primestomis" sąlygomis, t. y. jie iš tikrųjų neturi realios *autonomijos priimti sprendimus*. Galimybė derėtis dėl sąlygų vartotojui nesuteikiama, nes norėdamas naudotis produktu ar paslauga jis privalo arba sutikti, arba nesutikti. Dauguma šiuolaikinių internete veikiančių verslų pelną generuoja iš individų duomenų profiliavimo ir reklamos[623]. Nesutikimas su duomenų tvarkymu tokioje aplinkoje nėra realus pasirinkimas, nes dabartinėje rinkoje vartotojui būtų sunku

615 Solove, „Introduction: Privacy self-management and the consent dilemma", *supra note,* 36: 1886.

616 Daniel Le Métayer ir Julien Le Clainche, „From the protection of data to the protection of individuals: extending the application of non-discrimination principles", *European Data Protection: In Good Health?* (Springer, 2012), 315–329.

617 Solove, „Introduction: Privacy self-management and the consent dilemma", *supra note,* 36: 1886.

618 A. Acquisti ir J. Grossklags, „Privacy and rationality in individual decision making", *IEEE Security & Privacy* 3, 1 (2005): 26–33, https://doi.org/10.1109/MSP.2005.22.

619 Alessandro Acquisti ir kt., „What can behavioral economics teach us about privacy?", *Digital privacy* (Auerbach Publications, 2007), 369.

620 Richard H. Thaler ir Cass R. Sunstein, *Nudge* (Yale University Press, 2021).

621 Laura Brandimarte, Alessandro Acquisti ir George Loewenstein, „Misplaced confidences: Privacy and the control paradox", *Social psychological and personality science* 4, 3 (2013): 340–347.

622 Dan Ariely ir Simon Jones, *Predictably irrational* (HarperCollins New York, 2008).

623 Claudia Quelle, „Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection", *Privacy and Identity Management. Facing up to Next Steps,* sud. Anja Lehmann ir kt., t. 498, IFIP Advances in Information and Communication Technology (Cham: Springer International Publishing, 2016): 140–63, https://doi.org/10.1007/978-3-319-55783-0_11.

rasti alternatyvių prekių ar paslaugų teikėjų, kurie vadovautųsi duomenų apsaugai palankesniu verslo modeliu. Naudojimasis technologijomis yra toks svarbus, kad jų atsisakyti būtų ypač sunku. Pvz., asmuo šiais laikais neturėdamas išmaniojo telefono tikriausiai mažiau bendrautų su draugais, vien dėl to jis turėtų mažiau karjeros galimybių, jam sunkiau būtų užmegzti romantines pažintis, dažniau patirtų sunkumų darbe ar keliaudamas į užsienio valstybes ir pan.[624]

Ketvirta, žmonės susiduria su tiek daug duomenis tvarkančių subjektų, kad jiems nepakanka laiko tinkamai apsvarstyti, ar tuo atveju reikėtų duoti sutikimą, ar ne. Buvo atliktas tyrimas, kurio metu nustatyta, kad jei amerikiečiai skaitytų visas privatumo politikas, skelbiamas jų lankomose svetainėse, tais metais JAV ekonomikos produktyvumas sumažėtų apie 781 mlrd. dolerių[625]. Negana to, daugelis įmonių savo privatumo politikas nuolat keičia, taigi jas perskaityti kartą metuose neužtektų[626]. Šią problemą būtų galima spręsti grupuojant duomenų tvarkymą pagal tipus, tačiau dėl to didėtų rizika į vieną sudėti kelis duomenų tvarkymo tikslus, kas mažintų duomenų subjekto pasirinkimo galimybes, o tai iš esmės pažeistų BDAR sutikimo detalumo reikalavimą[627].

Penkta, net jeigu žmonės apie atskirus duomenų tvarkymo atvejus sprendimus priimtų racionaliai, jiems būtų sunku numatyti, kaip tie duomenys gali būti panaudojami (agreguojami) ateityje[628]. Agregavimas gali atskleisti platesnį informacijos kontekstą, iš kurio žmonių tapatybė gali būti nustatoma netgi tuomet, kai duomenys pateikiami anonimiškai[629]. BDAR profiliavimą pateisina reikalaudamas aiškaus duomenų subjekto sutikimo (angl. *explicit consent*). Vis dėlto, kaip jau aptarta, sutikimas yra gana problemiška privatumo apsaugos priemonė, nesuteikianti asmeniui realios savo privataus gyvenimo kontrolės dėl riboto racionalumo priimant sprendimus.

Šešta, nors sutikimas dėl duomenų tvarkymo dažnai turi ilgalaikių pasekmių, daugelis žmonių asmeninę informaciją iškeičia į trumpalaikę naudą, racionaliai negalėdami įvertinti, ar tokie mainai išties apsimoka. D. J. Solove'as sutikimą su duomenų tvarkymu palygina su bitės įkandimu: vienas iš esmės nepavojingas, bet šimtai gali baigtis mirtimi[630]. Kiekvienu papildomu sutikimu tvarkyti duomenis didžiųjų duomenų valdytojų serveriuose didinamas agreguojamų asmens duomenų kiekis, dėl to grėsmė asmens privatumui ir iš to išplaukiančiomis pasekmėmis per laiką tik didėja.

---

624 Tobias Matzner ir kt., „Do-It-yourself data protection—Empowerment or burden?", *Data protection on the move* (Springer, 2016): 277–305.

625 Aleecia M. McDonald ir Lorrie Faith Cranor, „The cost of reading privacy policies", *Isjlp* 4 (2008): 543.

626 Solove, „Introduction: Privacy self-management and the consent dilemma", *supra note,* 36: 1889.

627 BDAR, preambulės 43 punktas, „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679", 12.

628 Apie su agregavimu susijusias grėsmes žr. daugiau disertacijos 1.5.2 poskyrį.

629 Barbaro ir Zeller Jr, *supra note,* 593.

630 Solove, „Introduction: Privacy self-management and the consent dilemma", *supra note,* 36: 1891.

Taigi pagrindinė priežastis, dėl kurios savarankiško privatumo valdymo paradigma neveikia saugant teisę į privatumą, yra galios ir žinių asimetrija tarp sandorio šalių. Viena iš jų – vartotojai, kurie prieš duodami sutikimą neturi pakankamai nei laiko, nei žinių skaityti ir suvokti privatumo politikų, o esant sudėtingoms situacijoms sprendimus dažnai priima neracionaliai. Kita šalis – duomenis renkančios organizacijos. Jos turi išteklių samdyti marketingo ir teisės specialistus, kurie, pasinaudodami nepakankamais žmonių sprendimų priėmimo gebėjimais, juos paskatina sutikimą duoti, nei jo neduoti.

Viena iš alternatyvų savarankiško privatumo valdymo paradigmai yra reguliavimas, pagal kurį tam tikrus su privatumu susijusius pasirinkimus už vartotojus padaro teisės aktų leidėjai[631]. Tyrėjai šį reguliavimo būdą vadina *paternalistiniu* (angl. *paternalistic*)[632]. Plačiausia prasme paternalizmas gali būti suprantamas kaip individo pasirinkimo laisvės suvaržymas dėl jo paties gerovės[633].

Ryškūs paternalizmo pavyzdžiai šiais laikais yra normos, reikalaujančios vairuojant segėti saugos diržus, važiuojant motociklu dėvėti šalmą, taip pat draudimas vartoti narkotikus. Iš esmės paternalistinės ir dauguma specialiojo bepiločių orlaivių reguliavimo nuostatų, tarp jų, pvz., registracijos reikalavimas bei reikalavimas gaminti bepiločius orlaivius su nuotolinio identifikavimo ar geografinio orientavimo priedais. Specialiajame bepiločių orlaivių reguliavime savarankiško privatumo valdymo paradigma paremtas tik reikalavimas informuoti (gauti sutikimą). Pavyzdžiu taip pat galėtų būti BDAR nuostatos, leidžiančios asmens duomenis tvarkyti pagrindais, nesusijusiais su sutikimu ar sutartimi, t. y. tretiesiems asmenims naudingais pagrindais[634]. Tam, kad duomenys būtų renkami šiais pagrindais, duomenų subjekto sutikimo nereikia. Taigi šios teisės normos suvaržo individo pasirinkimo laisvę dėl trečiųjų asmenų ar visuomenės gerovės. Duomenų subjektas sutikimu taip pat negali tiesiog atsisakyti esminių duomenų tvarkymo principų, kuriuos numato BDAR 5 straipsnis. Vadinasi, šioje normoje numatyti principai, susiję su asmens duomenų tvarkymu, taip pat paternalistiniai. Atitinkamai paternalistinės yra nuostatos, taikančios pritaikytąją ir standartizuotąją duomenų apsaugą[635]. Net jeigu asmuo tam tikrais atvejais gali atsisakyti nuo pagal nutylėjimą (angl. *by default*) pritaikytos duomenų apsaugos, tokiomis nuostatomis bandoma paveikti duomenų subjekto sprendimą, todėl jos taip pat galėtų būti

631 *Ibid.,* 1897.

632 Žr. Kalle Grill, „Anti-paternalism and public health policy“ (KTH, 2009). Gerald Dworkin, „Defining Paternalism“, *New Perspectives on Paternalism and Health Care,* sud. Thomas Schramme, Library of Ethics and Applied Philosophy (Cham: Springer International Publishing, 2015), 17–29, https://doi.org/10.1007/978-3-319-17960-5_2. Emma C. Bullock, „A Normatively Neutral Definition of Paternalism“, *The Philosophical Quarterly* 65, 258 (2015 m. sausio 1 d.): 1–21, https://doi.org/10.1093/pq/pqu056. David Archard, „Paternalism defined“, *Analysis* 50, 1 (1990): 36–42.

633 *Ibid.,* 36–42.

634 BDAR, 6 straipsnio 1 dalies c–f punktai.

635 *Ibid.,* 25 straipsnis, preambulės 78 punktas.

vertinamos kaip paternalistinės[636].

BDAR rengėjai, remdamiesi paternalistiniais BDAR 6 straipsnio c–f punktuose nurodytais duomenų rinkimo pagrindais, taip pat naudodamiesi bendraisiais duomenų valdytojams taikomais duomenų tvarkymo principais bei pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimais, tarsi bando atsverti savarankiško privatumo valdymo trūkumus. Vadinasi, BDAR nesuteikia asmenims visiškos laisvės rinktis ar savo duomenis iškeisti į produktus ar paslaugas. Kai kuriomis nuostatomis individo pasirinkimas ribojamas siekiant apsaugoti jo paties arba visuomenės interesus. Nors BDAR yra paremtas savarankiško privatumo valdymo paradigma, jame svarbų vaidmenį atlieka ir paternalistinės nuostatos, kurių tikslas – apsaugoti duomenų subjektą nuo grėsmių, kurių šis galimai nenumatytų. Tokį patį poveikį turi ir specialiojo bepiločių orlaivių reguliavimo paternalistinės nuostatos. Pvz., nei bepiločio orlaivio valdytojas, nei stebimas asmuo patys nepriima sprendimo, ar nori, kad bepiločiai orlaiviai (ne)būtų gaminami su nuotolinio identifikavimo priedais, taip pat jie nesprendžia, ar bepiločio orlaivio valdytojui reikėtų registruotis. Už juos šiuos sprendimus priėmė įstatymų leidėjas – Europos Parlamentas. Nors šios nuostatos suvaržo individų savarankiško sprendimų priėmimo laisvę, bet jomis siekiama apginti visuomenės interesus, tokius kaip saugumas ir teisė į privatų gyvenimą.

Iš šio disertacijos tyrimo kyla klausimas: ar dabartinis specialusis bepiločių orlaivių reguliavimas ir bendrasis privatumo reguliavimas, kuriuose įtvirtintos paternalistinės nuostatos, atsveria trūkumus, atsirandančius dėl savarankiško privatumo valdymo? Pasak C. Quelle, savarankiško privatumo valdymo ir paternalistinių nuostatų pusiausvyros klausimas problemiškas, nes duomenų tvarkymo situacijų gali būti įvairių[637]. Kiekvienu atveju reikėtų svarstyti: (1) kokia informacija pateikiama vartotojui ir kaip ji perteikiama, (2) kitų variantų prieinamumą ir populiarumą rinkoje, (3) skaitmeninę aplinką, kurioje renkami ir naudojami duomenys, (4) bendrą socialinį ir ekonominį kontekstą, kuris turi įtakos, (5) kas duomenų subjektui įmanoma pagal esamą technologinę architektūrą ar kodą, (6) duomenų subjekto tikslus, norus, (7) kaip suvokiamos duomenų subjekto galimybės, tikslai

636 Richard H. Thaler ir Cass R. Sunstein, „Libertarian paternalism", *American economic review* 93, 2 (2003): 175–179; Gerald Dworkin, The theory and practice of autonomy (Cambridge University Press, 1988); Gerald Dworkin, „Defining Paternalism", *New Perspectives on Paternalism and Health Care,* sud. Thomas Schramme, Library of Ethics and Applied Philosophy (Cham: Springer International Publishing, 2015), 17–29, https://doi.org/10.1007/978-3-319-17960-5_2.

637 Claudia Quelle, „Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection", *Privacy and Identity Management. Facing up to Next Steps,* sud. Anja Lehmann ir kt., t. 498, IFIP Advances in Information and Communication Technology (Cham: Springer International Publishing, 2016), 140–163, https://doi.org/10.1007/978-3-319-55783-0_11. („If one has in mind a set of predefined interests, such as the interest in seclusion or the interest in secrecy, it is not problematic to conclude that the GDPR should require controllers to protect data subjects. In practice, however, the appropriateness of data flows is not clear-cut").

ir norai[638]. Vis dėlto esminė problema, susijusi su sutikimo reikalavimu naudojant bepiločius orlaivius, yra kitur. Plačiau apie tai kitame poskyryje.

4.6. Reguliavimo tobulinimo gairės per ribų valdymą

Atlikta analizė parodė, jog tiek BDAR, tiek specialusis bepiločių orlaivių reguliavimas yra paremtas stebimo asmens sutikimu. Tačiau realiai tai neužtikrina savarankiško asmens sprendimų priėmimo dėl įvairių priežasčių, *inter alia,* įgimto riboto žmonių racionalumo. Dėl to kylančias problemas BDAR bando spręsti paternalistinėmis nuostatomis, kuriose yra numatyti griežti reikalavimai duomenų valdytojų vykdomam duomenų tvarkymui. Atsvarą turėtų suteikti ir paternalistiniai prevencinės privatumo apsaugos reikalavimai, numatyti specialiajame bepiločių orlaivių reguliavime. Norint išsiaiškinti, ar tokie reikalavimai atsveria trūkumus, kurie atsiranda dėl savarankiško privatumo valdymo, reikėtų nagrinėti kiekvieną duomenų tvarkymo operaciją atskirai. Bepiločių orlaivių kontekste tokį tyrimą tikslinga būtų atlikti, jeigu duomenų subjektų sutikimą būtų taip lengva gauti kaip naršyti internete[639], tačiau, kaip parodė ankstesniuose disertacijos skyriuose atlikta analizė, sutikimą duomenims rinkti bepiločiu orlaiviu būtų ypač sudėtinga gauti[640]. Todėl vertinti pusiausvyrą tarp savarankiško privatumo valdymo ir paternalistinių priemonių bepiločių orlaivių kontekste nebūtina.

Sutikimo reikalavimas bepiločių orlaivių naudojimo atveju problemiškas visai kitu, gerokai paprastesniu aspektu – jį tiesiog sunku gauti. Realiame pasaulyje (priešingai nei internete) šiuo metu sunku įsivaizduoti mechanizmą, kuris visus bepiločio orlaivio skrydžio teritorijoje esančius žmones automatiškai informuotų apie planuojamą skrydį, o šiems nesutikus duomenų apie juos nerinktų. Kaip parodė ankstesniame disertacijos skyriuje atlikta specialiųjų bepiločių orlaivių reguliavimo šaltinių analizė[641], komplikuotą situaciją ICAO sprendžia pateikdama labai minimalius reikalavimus sutikimui, t. y. numato, kad sutikimas gali būti numanomas, tačiau vien šios sutikimo formos numatymas reglamentavime jau sudaro

638 *Ibid.,* 140–163; Antoinette Rouvroy ir Yves Poullet, „The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy“, *Reinventing data protection?* (Springer, 2009), 45–76; Orla Lynskey, The foundations of EU data protection law (Oxford University Press, 2015); Nadezhda Purtova, „Property rights in personal data“, *A European Perspective in Hugenholtz. B.(ed.), Information* (2011).

639 Žr. disertacijos 4.2.1 poskyrį (Nereikėtų atmesti tikimybės, kad ateityje gali rastis situacijos, kai į masinio sutikimo formas internete bus įtrauktas ir duomenų tvarkymas bepiločiais orlaiviais. Nepaspaudęs internetinės nuorodos į duomenų valdytojo duomenų tvarkymo politiką arba nuorodos „valdyti nustatymus“, vartotojas gali net nežinoti, jog į sutikimo formą įtrauktas ir sutikimas duomenis rinkti bepiločiais orlaiviais. Vis dėlto manytina, jog tokia žalinga praktika nacionalinių duomenų apsaugos institucijų ilgai neliktų nepastebėta).

640 Žr. disertacijos 4.2.1 poskyrį, 2.3.2 poskyrį.

641 Žr. disertacijos 2.3.2 poskyrį.

galimybę bepiločių orlaivių valdytojams piktnaudžiauti. JAV laikosi požiūrio, kad šiuo metu formaliai nustatyti reikalavimą informuoti ir gauti aplinkinių sutikimą nėra reikalo, todėl šios pareigos laikytis tik rekomenduoja ir tik tokiais atvejais, kai pats bepiločio orlaivio valdytojas mano, kad gali įsivežti į kitų individų asmeninę erdvę. ES reikalavimai, keliami sutikimui, labai griežti ir išsamūs, tačiau praktiškai neįgyvendinami vykdant skrydžius ten, kur yra didesni žmonių susibūrimai. Disertacijos autoriaus vertinimu, nė vienas šių reikalavimų neužtikrina pusiausvyros tarp pakankamos privatumo apsaugos ir bepiločių orlaivių technologinės pažangos. ES sutikimo reikalavimai per griežti, todėl slopina tolesnes bepiločių orlaivių inovacijas, o JAV ir ICAO – per laisvi, todėl neužtikrina pakankamos privatumo apsaugos.

Siekiant bepiločių orlaivių naudojimo pusiausvyros tarp teisės į privatų gyvenimą ir technologinės pažangos, tiktų vadovaujantis ankstesniame disertacijoje skyriuje aptarta ribų valdymo teorija. Joje visas dėmesys sutelkiamas į elgesio modelius, kuriuos norma išsaugoti (arba, atvirkščiai, neišsaugoti dėl didesnio gėrio). Šio reguliavimo modelio patrauklumą lemia paprastumas, taip pat jo teikiama galimybė visuomenei diskutuoti, kaip turėtų būti reguliuojamas privatumas viešojoje erdvėje. Savo ruožtu didesnis visuomenės įsitraukimas į sprendimų priėmimą ir ribų valdymo apsaugos regimybė turėtų skatinti visuomenės individualų bei grupinį savarankiškumą ir autonomiškumą, o tai turėtų padėti išvengti atšalimo efekto. Šios teorijos taikymas turėtų supaprastinti teisminius ginčus, kylančius dėl privatumo viešojoje erdvėje, ir ilgainiui turėtų užtikrinti, jog technologinė pažanga nebus apribota nepagrįstai[642]. Ši teorija iš esmės paternalistinė, nes kiekvieno elgesio šablono išsaugojimą (ar užgožimą) siūlo įtvirtinti privalomo pobūdžio įstatymų leidėjo (ar vietinės valdžios subjekto) priimtais teisės aktais, daugeliu atvejų nepaliekant galimybės individui sutikti arba nesutikti su įtvirtintu standartu.

Siekiant detaliau aptarti reguliavimo priemones, kuriomis šį pasiūlymą būtų galima įgyvendinti praktikoje, toliau vadovaujamasi ankstesniame disertacijos skyriuje apibrėžta reguliavimo sąvokos samprata[643]. Ji suprantama kaip susidedanti iš šešių pagrindinių teisinių santykių reguliavimo būdų: reguliavimo informuojant, savireguliavimo, jungtinio reguliavimo, standartizavimo, rinkos priemonių ir formalaus reguliavimo. Būdai, kurių reikėtų disertacijos autoriaus siūlomam reguliavimo modeliui įgyvendinti, yra formalus reguliavimas, reguliavimas informuojant ir standartizavimas. Vertėtų detaliau aptarti, kaip kiekvienas iš jų būtų pritaikomas įgyvendinant ribų valdymą ir paanalizuoti, kodėl netinka kiti reguliavimo būdai.

642 Žr. disertacijos 3.2.3 poskyrį.
643 Žr. disertacijos 2.1 poskyrį.

Iš pradžių bepiločių orlaivių reguliavimo per ribų valdymo teoriją veikimas būtų pagrįstas būtent *formaliu reguliavimu*. Šis reguliavimo būdas užtikrina, jog teismų praktikoje ir visuomenės gyvenime nekiltų klausimų dėl to, koks yra visuotinai priimtinas elgesio standartas atitinkamoje su privatumu susijusioje situacijoje. Disertacijos autoriaus nuomone, daugeliu atvejų pakankamus įgaliojimus įgyvendinti sprendimus, susijusius su bepiločių orlaivių skrydžių vykdymu ir informacijos rinkimu viešoje vietoje, turėtų vyriausybė ar savivaldybės. Tačiau ateityje, privatumo apsaugos problemai viešoje vietoje dėl bepiločių orlaivių naudojimo aštrėjant, tokius santykius būtų galima reguliuoti ir aukštesniu lygmeniu. Įstatymų leidėjas (parlamentas) galėtų priimti privalomo pobūdžio teisės aktą (įstatymą), kuriuo bendromis teisės normomis ribų valdymo mechanizmas būtų apibūdinamas ir įtvirtinamas nacionaliniu mastu. Įstatymas galėtų numatyti, kad saugotinus (ar slopintinus) elgesio šablonus nustato vykdomoji valdžia (vyriausybė) atskiru nutarimu arba vietinės valdžios institucijos. Atvejus, kada santykius tarp bepiločių orlaivių valdytojų ir visuomenės gali tekti reguliuoti aiškiau galima įsivaizduoti per konkrečius pavyzdžius. Iliustraciniais tikslais žemiau pateikiamos dvi situacijos, galimos netolimoje ateityje.

Situacija Nr. 1	
Mažmeninės prekybos asociacija Lietuvoje, siekdama pagerinti parduotuvių išsidėstymą ir reklamos efektyvumą, norėtų naudoti bepiločius orlaivius su dirbtiniu intelektu ir mašininio mokymo algoritmais. Bepiločiai orlaiviai skraidytų virš pagrindinių miesto prekybos zonų, fiksuotų pirkėjų judėjimo srautus, laiką, praleistą prie įvairių parduotuvių, ir jų sąveiką su reklamomis. Surinkti duomenys būtų perduodami dirbtinio intelekto modeliams, kurie pateiktų rekomendacijas dėl optimalios parduotuvių išsidėstymo strategijos, reklamos vietų ir turinio.	
Problema	Mažmeninės prekybos asociacija šios idėjos įgyvendinti negali, nes pagal BDAR norint vykdyti tokio pobūdžio stebėseną viešoje vietoje, reikėtų gauti visų stebimų individų sutikimus.
Sprendimas	Vietos valdžios institucija galėtų nustatyti leidimų stebėsenai viešoje vietoje išdavimo tvarką. Pagal šią tvarką, subjektai, planuojantys vykdyti stebėseną bepiločiais orlaiviais, galėtų prašyti vietinės valdžios išduoti leidimus vykdyti stebėseną. Leidimų stebėsenai viešoje vietoje išdavimo tvarka galėtų numatyti, kad su paraiška privaloma pateikti užpildytą PDAV. Tokiu būdu pareiškėjas galėtų iš anksto pagrįsti, kodėl jo vykdoma stebėsena pernelyg nepažeidžia aplinkinių privatumo arba kodėl įsiveržimas į asmenų privatų gyvenimą būtų pateisinamas. Vietos valdžios institucijos aprašyta tvarka galėtų nustatyti kriterijus leidimų išdavimui, vadovaudamasi ribų valdymo teorija. Išduotas leidimas mažmeninės prekybos asociacijai galėtų būti pagrindas rinkti duomenis pagal BDAR 6 straipsnio 2 dalį (nacionalinis teisės aktas kaip pagrindas duomenis rinkti bepiločiu orlaiviu)[644].

644 Aiškumo dėlei vertėtų paminėti, kad visiškai autonominiams skrydžiams bepiločiais orlaiviais visais atvejais reikalingas nacionalinės aviacijos organizacijos leidimas (specialiosios kategorijos skrydžiai). Su paraiška gauti leidimą bepiločio orlaivio valdytojai privalo pateikti veiklos rizikos vertinimą, atliktą pagal Reglamento (ES) 2019/947 11 straipsnio reikalavimus, tačiau, kaip minėta disertacijos 2.3.6. poskyryje, veiklos rizikos vertinimas bepiločių orlaivių operatorių neįpareigoja įvertinti rizikos privatumui. Žr. Viešosios įstaigos Transporto kompetencijų agentūros direktoriaus 2021 m. lapkričio 5 d. įsakymas Nr. 2-134 „Dėl leidimų vykdyti specialiosios kategorijos skrydžius naudojant bepiločio orlaivio sistemą išdavimo tvarkos aprašo patvirtininimo“ (Suvestinė redakcija nuo 2023-12-02).

<table>
<tr><th colspan="2">Situacija Nr. 2</th></tr>
<tr><td colspan="2">Didžiųjų miestų savivaldybės, bendradarbiaudamos su technologijų bendrovėmis, planuoja diegti išmaniosios miesto (Smart City) technologijas, siekdamos pagerinti miestų gyventojų gyvenimo kokybę, padidinti saugumą ir skatinti ekonomikos augimą. Viena iš pagrindinių iniciatyvų – naudojant bepiločius orlaivius surinkti duomenis apie miesto infrastruktūros naudojimą, gyventojų judėjimą ir elgesio modelius. Maži, nepastebimi bepiločiai orlaiviai, aprūpinti pažangiais jutikliais ir dirbtinio intelekto algoritmais, skraidys virš miesto teritorijų ir rinktų duomenis apie transporto srautus ir eismo sąlygas, pėsčiųjų ir dviratininkų judėjimo maršrutus, viešojo transporto naudojimą ir sustojimų dažnumą, viešųjų erdvių ir parkų lankomumą, oro kokybę ir aplinkos taršą skirtingose miesto vietose, pastatų energetinį efektyvumą ir naudojamą energiją. Surinkti duomenys būtų apdorojami dirbtinio intelekto sistemose, kurios analizuotų informaciją realiu laiku. Šios sistemos pateiktų įžvalgas ir rekomendacijas, kurios padėtų miesto valdžios institucijoms ir verslo subjektams kurti naujus produktus ir paslaugas.</td></tr>
<tr><td>Problema</td><td>Didžiųjų miestų savivaldybės idėjos įgyvendinti negali, nes pagal BDAR norint vykdyti tokio pobūdžio stebėseną viešoje vietoje, reikėtų gauti visų stebimų individų sutikimus.
Taip pat nuolatinė populiacijos stebėsena bepiločiais orlaiviais kelia akivaizdžią grėsmę piliečių privatumui. Didžiųjų miestų savivaldybės įgyvendinusios tokį sprendimą poįstatyminiais teisės aktais rizikuotų teisminiais ginčais dėl teisės į privatų gyvenimą pažeidimo.</td></tr>
<tr><td>Sprendimas</td><td>Pagrindu tokiu atveju rinkti duomenis pagal BDAR 6 straipsnio 2 dalį galėtų būti nacionalinis teisės aktas. Tokiu atveju visų stebimų individų stebimų individų sutikimus gauti nebūtina.
Valstybė galėtų nacionaliniu mastu priimti įstatymą, kuriuo vadovaujantis ribų valdymo teorija būtų nustatyti saugotini (ar slopintini) žmonių elgesio šablonai. Tuo tarpu savivaldybės poįstatyminiais teisės aktais galėtų detaliau įtvirtinti kokiomis priemonėmis toks elgesio šablonas išsaugomas arba pagrįstai apribojamas. Įstatymas galėtų, pavyzdžiui, numatyti, kad saugotini elgesio šablonai yra:
- Asmeninis laikas viešuosiuose parkuose. Įstatymas galėtų numatyti, jog laisvalaikio leidimas miestų viešuosiuose parkuose yra svarbus, nes ten žmonės bendrauja vieni su kitais privačiomis temomis, nori atsipalaiduoti žinodami, kad nebus nuolat stebimi. Poįstatyminiais teisės aktais savivaldybės gali nustatyti, kaip konkrečiai šis elgesio šablonas bus išsaugotas. Pavyzdžiui, skrydžiai bepiločiais orlaiviais viešųjų parkų zonose gali būti vykdomi ne žemesniame kaip 150 m aukštyje. Arba skrydžiai bepiločiais orlaiviais virš parkų iš viso negali būti vykdomi. Arba virš parkų skrydžiai negali būti vykdomi išmaniosios miesto infrastruktūros bepiločiais orlaiviais.
- Dalyvavimas viešuose kultūriniuose ir religiniuose renginiuose. Įstatymas galėtų numatyti, kad, pvz., koncertuose, spektakliuose ar pamaldose, žmonės turi būti apsaugoti nuo nuolatinio stebėjimo, nes tokio pobūdžio renginiuose žmonės taip pat turi pagrįstą lūkestį, kad bus stebimi tik esant būtinybei užtikrinti saugumą. Savivaldybės poįstatyminiais teisės aktais gali nustatyti konkrečius stebėjimo reikalavimus, pavyzdžiui, kad bepiločių orlaivių skrydžiai išmanaus miesto infrastruktūros bepiločiais negalimi kultūrinių ir religinių renginių metu.
- Asmenų teisė kalbėtis su draugais, šeimos nariais ar kolegomis viešose vietose. Įstatymas galėtų numatyti, jog, pvz., kavinių terasose ar viešosiose aikštėse, aktyvi stebėsena bepiločiais orlaiviais neturėtų būti vykdoma. Savivaldybės galėtų nustatyti, kad bepiločių orlaivių naudojimas tokiose vietose būtų ribotas arba visiškai uždraustas.
Įstatymas taip pat galėtų numatyti atvejus, kada saugotinus elgesio šablonus galima slopinti taikant didesnio įsiveržimo lygio stebėseną bepiločiais orlaiviais vardan didesnio gėrio, pavyzdžiui:
- Transporto priemonių eismo stebėjimas saugumo užtikrinimo tikslu. Siekiant užtikrinti eismo saugumą, transporto priemonių greičio stebėjimas bepiločiais orlaiviais gali būti leidžiamas. Savivaldybės gali nustatyti konkrečias taisykles, pagal kurias bepiločiai orlaiviai gali fiksuoti transporto priemonių greitį ir perduoti šiuos duomenis teisėsaugos institucijoms, siekiant sumažinti greičio viršijimo atvejus ir pagerinti eismo sąlygas mieste.</td></tr>
</table>

	- **Viešųjų erdvių, viešųjų renginių stebėjimas saugumo užtikrinimo tikslu.** Visų arba kai kurių viešųjų erdvių stebėjimas siekiant užtikrinti žmonių saugumą gali būti leidžiamas. Savivaldybės savo teisės aktuose galėtų papildomai detalizuoti, kad tam tikrose vietose ar tam tikro tipo renginių metu gali būti naudojami atitinkamo tipo išmaniojo miesto infrastruktūros bepiločiai orlaiviai. Arba, kad bepiločiai orlaiviai stebėseną tokiais atvejais vykdo periodiniais praskridimais. Arba, kad bepiločiai atitinkamose teritorijose gali naudoti tik tam tikro tipo jutiklius. - **Sveikatos apsaugos užtikrinimo tikslu.** Norint pagerinti sveikatos priežiūros paslaugų prieinamumą ir efektyvumą, įstatymu gali būti nuspręsta leisti naudoti ir privatumą stipriai varžančius bepiločius orlaivius, fiksuojančius sveikatos sutrikimų požymius, pvz. širdies smūgio simptomus, alpimo atvejus ar kitas kritines sveikatos būkles. Savivaldybės poįstatyminiais teisės aktais, vėlgi, galėtų numatyti tam tikrus technologinius apribojimus duomenų rinkimui, arba pažangesnį duomenų rinkimą įgalinančius sprendimus priklausomai nuo įstatymo formuluotės.

Ankstesniame disertacijos skyriuje jau minėta, jog taikant ribų valdymo teoriją būtų skatinama visuomenė įsitraukti į teisinę diskusiją dėl reikšmingų elgesio modelių, kuriuos ji norėtų apsaugoti. Tai turėtų skatinti visuomenės individualų bei grupinį savarankiškumą ir autonomiškumą, padėtų išvengti atšalimo efekto[645]. Galimybę visuomenei dalyvauti diskusijoje užtikrina bet kuris teisėkūros procesas demokratinėse santvarkose. Formalaus reguliavimo procesas prasideda nuo teisinių idėjų, kurios teisėkūros procese yra perdirbamos į teisės normas[646]. Tam, kad Lietuvoje idėja taptų teisės aktu, įstatymo projektą Seime turėtų inicijuoti vienas iš LR Konstitucijos 68 straipsnyje nurodytų subjektų. Įregistruotas naujas projektas toliau siunčiamas atitinkamiems Seimo komitetams ir komisijoms, kurie jį patikrina ir parengia derinimui, *inter alia,* su visuomeninėmis organizacijomis, socialinėmis grupėmis, taip pat skelbti spaudoje, internete, kad visuomenė susipažintų[647]. Būtent šiame teisės akto rengimo etape visuomenė turėtų galimybę įsitraukti į teisinę diskusiją dėl saugotinų ar slopintinų elgesio modelių.

Pastebėtina, jog Lietuvoje ministerijų rengiami įsakymai iš anksto nėra derinami su visuomene tokia pačia tvarka kaip įstatymų projektai, todėl bepiločių orlaivių reguliavimą per ribų valdymo teoriją disertacijos autorius rekomenduotų įgyvendinti per įstatymų leidžiamąją valdžią. Vykdomoji valdžia įsakymus dėl ribų valdymo mechanizmų viešojoje erdvėje turėtų priimti tik išimtiniais atvejais, kai situacija reikalauja greito sprendimo. Siekiant į diskusiją įtraukti visuomenę, Vyriausybės sureguliuotus bepiločių orlaivių valdytojų ir visuomenės santykius, vėliau reikėtų perkelti į įstatymus.

645 Žr. disertacijos 3.2.3 poskyrį.
646 Vaišvila, *supra note,* 244: 213, 223.
647 *Ibid.,* 229.

Kiti reguliavimo būdai. *Reguliavimas informuojant* disertacijos autoriaus siūlomai teorijai būtų taikomas netiesiogiai. Tam, kad individai galėtų koreguoti savo elgesį pagal teisės aktais pakeistas privatumo ribas viešojoje erdvėje, ribų valdymo teorija paremtas formalus reguliavimas turėtų nustatyti informavimo pareigą. Tokį reikalavimą turėtų įgyvendinti valdžios institucijos, jos apie naujus ribų valdymo mechanizmus įgyvendinančius įstatymus skelbtų žiniasklaidoje. Taip pat informaciniais ženklais praneštų praeiviams apie naujai įsigaliojusį ribų valdymo mechanizmą atitinkamoje teritorijoje.

Standartizavimas kaip reguliavimo būdas reiškia, kad formalaus reguliavimo galią turinti institucija suteikia mandatą vyriausybinei organizacijai kurti rekomendacinio pobūdžio standartus. Į standartų kūrimo procesą organizacija įtraukia suinteresuotus fizinius ir juridinius asmenis. Pvz., Lietuvoje standartizavimą duomenų apsaugos srityje atlieka Valstybinė duomenų apsaugos inspekcija (toliau – VDAI). Disertacijos autoriaus vertinimu, šį reguliavimo būdą bepiločių orlaivių atveju reikėtų taikyti, kad formalus reguliavimas būtų labiau suprantamas visuomenei ir verslo subjektams. Gairėse ir rekomendacijose galėtų būti pateikiami praktiniai formalaus reguliavimo taikymo scenarijai, be to, jas galėtų papildyti rinkos veikėjai savo patirtimi, tad į sprendimų priėmimą būtų įtraukiama ir visuomenė.

Technologijoms nuolat vystantis *savireguliavimo* svarba didėja, nes formalus teisinis reguliavimas gerokai atsilieka nuo technologinės pažangos. Priežastys, kodėl laiku nepriimamas formalus reguliavimas, galimos įvairios. Valdžios institucijoms gali nepakakti žinių, kad sureguliuotų naują reiškinį, taip pat gali būti delsiama vengiant nepagrįtai suvaržyti technologinį progresą. Gali būti, kad santykių sureguliavimas per brangiai kainuotų arba, valstybės institucijų vertinimu, santykių nereguliavimas nekelia didelio pavojaus visuomenei. Savireguliavimą dažniausiai įgyvendina rinkos veikėjus vienijančios nevyriausybinės organizacijos, jos patvirtina gaires, reguliuojančias santykį, ar standartus, rengia mokymus. Lietuvos bepiločių orlaivių rinkoje tokia galėtų būti, pvz., 2014 m. įsteigta Lietuvos bepiločių orlaivių naudotojų asociacija. Duomenų apsaugos srityje Lietuvoje veikia 2019 m. įsteigta Asmens privatumo gynimo ir duomenų apsaugos asociacija (APGIDA). Nevyriausybinės organizacijos prisidėdamos prie siūlomo bepiločių orlaivių reguliavimo, taikant ribų valdymo teoriją, galėtų įsitraukti nebent į formalaus reguliavimo procesą ir teikti savo asociacijos narių pasiūlymus. Savireguliavimo sprendimai, taikant ribų valdymo teoriją, nebūtų veiksmingi, nes privačios įmonės, netgi nusistačiusios ribų valdymo viešoje vietoje mechanizmus, neturėtų teisinio pagrindo duomenis tvarkyti be duomenų subjektų sutikimų, o šiuos bepiločių orlaivių kontekste, kaip jau aptarta, gauti būtų sudėtinga.

Jungtinio reguliavimo esmė yra teisės aktais nustatyti abstrakčius tikslus tam tikroje srityje pripažintiems nevyriausybiniams subjektams (ūkio subjektams, socialiniams partneriams, nevyriausybinėms organizacijoms ar asociacijoms), kuriais vadovaudamiesi jie patys nusistato standartus. Toks reguliavimo būdas, taikant ribų valdymo teoriją, taip pat nebūtų priimtinas dėl

abstraktumo. Saugotini (atsisakytini) elgesio šablonai ir ribų valdymo mechanizmai turėtų būti nustatyti labai konkrečiai. Kitaip visuomenėje ir teismų praktikoje būtų daug diskusijų dėl taikytino ribų valdymo mechanizmo, o duomenų valdytojams kiltų klausimų, ar konkrečiu atveju nenusižengia BDAR reikalavimams.

Galiausiai *rinkos priemonės* yra instrumentai, kuriais naudodamasi valstybė rinkos žaidėjams teikia pozityvią arba negatyvią piniginę paskatą, nustato pagrindines žaidimo taisykles (teikiamos kompensacijos, parduodami leidimai, mokesčiai, rinkliavos, nuosavybės ir atsakomybės taisyklės, licencijos, kvotos ir pan.). Disertacijos autoriaus vertinimu, šios priemonės labiau tinkamos tokiose teisės srityse kaip aplinkosauga[648]. Kaip jos galėtų būti pritaikytos privatumo sričiai, apskritai sunku įsivaizduoti, todėl ši reguliavimo priemonė privatumo apsaugai nuo bepiločių orlaivių keliamų grėsmių nebūtų tinkama.

Atlikta analizė atskleidė, jog savarankiškas privatumo valdymas, paremtas individo sutikimu, turi trūkumų. Duodami sutikimą tvarkyti duomenis žmonės dažnai nesupranta realių savo pasirinkimo pasekmių arba jas supranta kiek iškreiptai dėl įgimto riboto racionalumo. Taip pat galima teigti, jog individai šių dienų rinkos sąlygomis neturi realios autonomijos priimti sprendimus, nes verslo modelių, pagal kuriuos būtų renkama mažiau duomenų, ekonomikoje tiesiog nėra. Žmonės neturi laiko skaityti privatumo politikų, tiksliai nenumato ilgalaikių duomenų tvarkymo ir derinimo tarpusavyje (agregavimo) pasekmių. Viena iš mokslinėje literatūroje siūlomų išeičių yra paternalistinis reguliavimas, kuriuo iš esmės suvaržoma individo pasirinkimo laisvė dėl jo paties gerovės. Paternalistinių nuostatų gausu įvairiuose šiuolaikiniuose teisės aktuose, tarp jų ir BDAR, ir specialiajame bepiločių orlaivių reguliavime. Disertacijos autoriaus siūlomas bepiločių orlaivių reguliavimo modelis taip pat paternalistinis. Jis paremtas ne sutikimu, o privalomo pobūdžio elgesio taisyklėmis, pagrįstomis formaliu reguliavimu. Šis reguliavimo modelis patrauklus tuo, kad yra paprastas. Jo taikymas galėtų palengvinti teismų darbą, o diskutuojant, kaip turėtų būti reguliuojamas privatumas viešojoje erdvėje, galėtų įsitraukti ir visuomenė. Disertacijos autoriaus vertinimu, siūlomas reguliavimas galėtų būti įgyvendintas per formalų reguliavimą, reguliavimą informuojant ir standartizavimą.

---

648 Maryam Mazaheri ir kt., „Market-Based Instruments and Sustainable Innovation: A Systematic Literature Review and Critique“, *Journal of Cleaner Production* 373 (2022): 133947, https://doi.org/10.1016/j.jclepro.2022.133947.

IŠVADOS

Apibendrindamas atliktą mokslinį tyrimą disertacijos autorius konstatuoja, kad įvade nurodytas disertacinio tyrimo tikslas pasiektas, išsikelti uždaviniai įgyvendinti, o ginamieji teiginiai patvirtinti. Tai pagrindžia toliau pateikiamos tyrimo išvados:

1. Disertacijoje atliktas tyrimas atskleidė, jog bepiločiai orlaiviai grėsmę privatumui kelia per tokius pažeidimus kaip stebėsena, agregavimas, identifikavimas, saugumo neužtikrinimas ir atidengimas. Šių pažeidimų grėsmė kyla, nes bepiločių orlaivių technologija turi išskirtinių savybių, kurių neturi nė viena iki šiol prieinama stebėsenos priemonė. Tai tokios savybės kaip didelis panaudojimo mastas, stebėjimo intensyvumas, stebėjimo kampų įvairovė, galimybė tapti ginklu ir nepastebimumas. Kaip parodė atliktas tyrimas, išskirtinės bepiločių orlaivių galimybės įgalina tiek valstybes, tiek didelę galią rinkoje turinčius subjektus kurti infrastruktūrą oportunistiniam informacijos rinkimui realiame pasaulyje, todėl tinkamai nereglamentuojant bepiločių orlaivių naudojimo galimas atšalimo efektas, t. y. nepageidaujami žmonių psichikos pokyčiai, socialinių grupių ir skirtingų visuomenės sluoksnių elgsenos pakitimai į blogąją pusę, grėsmė demokratinės santvarkos stabilumui.

2. Iš nagrinėtų specialiųjų bepiločių orlaivių reguliavimo šaltinių, kuriuos yra priėmę ICAO, JARUS, ES ir JAV, matyti, jog *expressis verbis* privatumo apsaugą įtvirtina tik ES bepiločių orlaivių reglamentai. Vis dėlto tai nereiškia, jog kiti nagrinėti šaltiniai privatumo apsaugos priemonių nenumato – juose apsaugos priemonės įtvirtintos netiesiogiai. Atlikta analizė parodė, jog dabartiniuose specialiuosiuose bepiločių orlaivių teisės aktuose egzistuoja šios prevencinės priemonės, kurios galėtų padėti išvengti privatumo pažeidimų: (a) reikalavimas laikytis atstumo; (b) reikalavimas informuoti / gauti sutikimą; (c) registracijos reikalavimas; (d) reikalavimas kaupti įrašus; (e) kvalifikacijos reikalavimus bepiločių orlaivių pilotams; (f) reikalavimai atlikti rizikos vertinimą; (g) nuotolinio identifikavimo priedai; (h) geografinio orientavimo priedai (geografinis apribojimas); (i) duomenų perdavimo ryšio linijos saugumo užtikrinimas; (j) reikalavimas bepiločius orlaivius gaminti su žibintais. Disertacijos autoriaus vertinimu, visos aptartos priemonės vienokiu ar kitokiu būdu teoriškai galėtų sumažinti privatumo pažeidimų tikimybę, tačiau daugelis jų šiuo metu realios prevencijos neužtikrina dėl reglamentuojančiuose nuostatuose esančių trūkumų ir nepakankamo privatumą saugančių technologijų išsivystymo.

3. Atlikus privatumo viešojoje erdvėje mokslinės literatūros analizę buvo identifikuotos trys moksliniame diskurse vyraujančios teorijos, kurių pagrindu užsienio autoriai siūlo reguliuoti privatumo ribas viešojoje erdvėje: (i) *kontekstinio integralumo teorija,* (ii) *visuomeninės reikšmės teorija* ir (iii) *ribų valdymo teorija*. Kiekviena jų buvo analizuojama, siekiant nustatyti, ar kuri nors iš jų sukurtų pusiausvyrą tarp privatumo viešojoje erdvėje ir technologinės pažangos. Atliktas

tyrimas parodė, jog *kontekstinio integralumo teorija* nesuteiktų pakankamos privatumo apsaugos nuo pažeidimų, kuriuos gali sukelti nedidelių bepiločių orlaivių naudojimas. Ją taikant nagrinėjamas jau surinktos informacijos tolesnio perleidimo ir lyginimo teisėtumas, tačiau pats duomenų rinkimo faktas nėra svarbus, o bepiločių orlaivių kontekste kaip tik sureguliuoti duomenų rinkimo teisėtumą būtų svarbiausia. Disertacijos autoriaus vertinimu, *visuomeninės reikšmės teorija* taip pat nesuteiktų tinkamos apsaugos privatumui. Ją taikant aiškintis, kuri teisė viršesnė – teisė į privatumą ar teisė į saviraišką, teismai būtų per daug apkraunami. Šis reguliavimo modelis beveik nesuteikia jokios pridėtinės vertės, palyginti su pasenusia dvinare teorija, kuriai svarbiausia, ar informacija buvo surinkta viešojoje ar privačioje erdvėje, t. y. teritorinė viešosios ir privačios erdvės perskyra. Galiausiai *ribų valdymo teorijos* taikymas, disertacijos autoriaus nuomone, turėtų supaprastinti įstatymų leidybos procesą, palengvinti teisminius ginčus, kylančius dėl bepiločių orlaivių naudojimo, pernelyg nesuvaržyti bepiločių orlaivių technologinio vystymosi. Šio modelio taikymas taip pat turėtų skatinti visuomenės įsitraukimą į sprendimų priėmimą teisinio reguliavimo procese, skatinti visuomenės individualų bei grupinį savarankiškumą, autonomiškumą, todėl atitinkamai turėtų padėti išvengti atšalimo efekto.

4. EŽTT ir LAT praktikos, susijusios su privatumo ribomis viešojoje erdvėje, analizė atskleidė, jog bylų, nagrinėjančių bepiločių orlaivių naudojimą, teismai iki šiol nėra sprendę. Kasacinio teismo jurisprudencijoje su privatumu susijusių bylų apskritai nėra daug, jose negausu universalaus taikymo teisės taisyklių, todėl iš esamos praktikos daryti išvadas apie tolesnę Lietuvos teismų sprendimų motyvaciją, iškilus byloms bepiločių kontekste, būtų pernelyg drąsu. Iš EŽTT jurisprudencijos, kuria privalo vadovautis ir Lietuvos teismai, matyti reikšmingai skirtingas privatumo viešojoje erdvėje ribų vertinimas, priklausomai nuo to, koks subjektas vykdo stebėseną – privatus asmuo ar valdžios institucija. Pagal suformuotą praktiką privačių subjektų bepiločiais orlaiviais vykdoma stebėsena turėtų būti kur kas labiau prižiūrima ir reguliuojama, tačiau esama praktika pernelyg abstrakti, kad ja teisėjai bepiločių orlaivių naudojimo ir privatumo santykio bylose galėtų vadovautis be papildomo teorinio pagrindo. Tokį teorinį pagrindą suteikia siūloma ribų valdymo teorija, kuri būtų suderinama su EŽTT jau suformuotomis universalaus taikymo taisyklėmis. Valdžios institucijų viešojoje erdvėje vykdoma stebėsena bepiločiais orlaiviais pagal suformuotą EŽTT praktiką beveik nebūtų ribojama dėl neseniai priimto masinės stebėsenos režimui palankaus sprendimo byloje „Big Brother Watch and Others v. the United Kingdom“, kuriuo remiantis valstybėms suteikiama plati diskrecija pasirinkti, kiek bus varžomas asmenų privatumas siekiant nacionalinio saugumo. Disertacijos autoriaus manymu, slapta masinė stebėsena, nesvarbu, kas ją vykdo, valdžios institucijos ar privatūs asmenys, iš materialiosios teisės perspektyvos, visais atvejais būtų nesuderinama su ribų valdymo teorija ir lemtų privatumo pažeidimus, nes stebimi asmenys, nežinodami apie jų atžvilgiu vykdomą stebėseną, negali keisti savo elgesio. Manytina, jog šiuo metu vienintelis dalykas, galintis sustabdyti slaptos bepiločiais orlaiviais vykdomos stebėsenos

taikymą, yra stipri tarptautinė arba nacionalinė politinė valia atsisakyti masinės valstybės institucijų vykdomos stebėsenos. Kaip parodė atliktas tyrimas, šiuo požiūriu Lietuvos teisės aktai, nors ir kritikuojami Lietuvos teismų, keičiami privatumui nepalankia linkme.

5. Kaip parodė atlikta ES duomenų teisės aktų analizė, į BDAR reguliavimo sritį bepiločiai orlaiviai patenka, nes tai įrankis duomenims rinkti. BDAR bepiločių orlaivių vykdomam duomenų rinkimui nebūtų taikomas tik tais atvejais, kai iš surinktos medžiagos asmenų neįmanoma identifikuoti, arba tada, kai duomenys pateikiami anonimiškai. Iš teisėtų duomenų tvarkymo pagrindų, kuriais galėtų vadovautis bepiločių orlaivių valdytojai, disertacijos autoriaus nuomone, labiausiai tikėtini yra duomenų subjekto sutikimas (BDAR 6 straipsnio 1 dalies a punktas) ir „teisėtas interesas" (BDAR 6 straipsnio 1 dalies f punktas). Disertacijos autorius identifikavo dar vieną realų duomenų bepiločiais orlaiviais rinkimo pagrindą, kurio *expressis verbis* BDAR nenumato, tai – nacionalinis teisės aktas. Atlikta analizė parodė, jog pagal ESTT praktiką, suformuotą stacionarių CCTV kamerų kontekste, net ir paprasti vartotojai, vykdydami skrydį viešoje vietoje, turėtų gauti aplinkinių sutikimą. Vis dėlto, disertacijos autoriaus vertinimu, BDAR nuostatų tikriausiai nereikėtų taikyti vidutiniams vartotojams, vykdantiems skrydžius asmeniniais tikslais, todėl šia ESTT praktika vadovautis nebūtų tikslinga. Vertinant BDAR siūlomas privatumo apsaugos priemones prieita prie išvados, jog didžiausią naudą suteikia šifravimo sprendimai ir poveikio duomenų apsaugai vertinimai. Kaip vienas iš šifravimo sprendimų, atskirai aptartas anonimiškumas, kuriuo apdoroti duomenys į BDAR taikymo sritį nepatektų. Tiesa, šiuo metu anonimizavimo technologija nėra pakankamai išsivysčiusi, todėl negalėtų būti plačiai taikoma. Taip pat kritikuotina, jog dabartiniai teisės aktai nenumato anonimizuotų duomenų saugojimo termino, o tai sudaro dingstis piktnaudžiauti. Kitos BDAR numatytos privatumo apsaugos garantijos abstraktesnio pobūdžio, bet taip pat reikšmingai prisideda prie privatumo apsaugos, nes veikia kaip standartizavimo šaltinis, kuriuo vadovaudamiesi bepiločių orlaivių rinkos dalyviai gali užsiimti kryptinga savireguliacija. Taigi sutikimas – pagrindinis ES duomenų apsaugos režimo ramstis, todėl BDAR, neskaitant kai kurių naudingų numatytų konkrečių privatumo apsaugos priemonių, privatumo apsauga, paremta *savarankiško privatumo valdymo* paradigma, būtų neveiksminga privatumo apsaugai bepiločių orlaivių naudojimo kontekste.

6. Savarankiškas privatumo valdymas, paremtas individo sutikimu, turi trūkumų. Duodami sutikimą tvarkyti duomenis, žmonės dažnai nesupranta realių savo pasirinkimo pasekmių arba jas supranta kiek iškreiptai dėl įgimto riboto racionalumo. Taip pat galima teigti, jog individai šių dienų rinkos sąlygomis neturi realios autonomijos priimti sprendimus, nes verslo modelių, pagal kuriuos būtų renkama mažiau duomenų, ekonomikoje tiesiog nėra, Žmonės taip pat neturi laiko skaityti privatumo politikų, tiksliai nenumato ilgalaikių duomenų tvarkymo ir derinimo tarpusavyje (agregavimo) pasekmių. Viena mokslinėje literatūroje siūlomų išeičių – paternalistinis reguliavimas, kuriuo iš esmės suvaržoma

taikymą, yra stipri tarptautinė arba nacionalinė politinė valia atsisakyti masinės valstybės institucijų vykdomos stebėsenos. Kaip parodė atliktas tyrimas, šiuo požiūriu Lietuvos teisės aktai, nors ir kritikuojami Lietuvos teismų, keičiami privatumui nepalankia linkme.

5. Kaip parodė atlikta ES duomenų teisės aktų analizė, į BDAR reguliavimo sritį bepiločiai orlaiviai patenka, nes tai įrankis duomenims rinkti. BDAR bepiločių orlaivių vykdomam duomenų rinkimui nebūtų taikomas tik tais atvejais, kai iš surinktos medžiagos asmenų neįmanoma identifikuoti, arba tada, kai duomenys pateikiami anonimiškai. Iš teisėtų duomenų tvarkymo pagrindų, kuriais galėtų vadovautis bepiločių orlaivių valdytojai, disertacijos autoriaus nuomone, labiausiai tikėtini yra duomenų subjekto sutikimas (BDAR 6 straipsnio 1 dalies a punktas) ir „teisėtas interesas" (BDAR 6 straipsnio 1 dalies f punktas). Disertacijos autorius identifikavo dar vieną realų duomenų bepiločiais orlaiviais rinkimo pagrindą, kurio *expressis verbis* BDAR nenumato, tai – nacionalinis teisės aktas. Atlikta analizė parodė, jog pagal ESTT praktiką, suformuotą stacionarių CCTV kamerų kontekste, net ir paprasti vartotojai, vykdydami skrydį viešoje vietoje, turėtų gauti aplinkinių sutikimą. Vis dėlto, disertacijos autoriaus vertinimu, BDAR nuostatų tikriausiai nereikėtų taikyti vidutiniams vartotojams, vykdantiems skrydžius asmeniniais tikslais, todėl šia ESTT praktika vadovautis nebūtų tikslinga. Vertinant BDAR siūlomas privatumo apsaugos priemones prieita prie išvados, jog didžiausią naudą suteikia šifravimo sprendimai ir poveikio duomenų apsaugai vertinimai. Kaip vienas iš šifravimo sprendimų, atskirai aptartas anonimiškumas, kuriuo apdoroti duomenys į BDAR taikymo sritį nepatektų. Tiesa, šiuo metu anonimizavimo technologija nėra pakankamai išsivysčiusi, todėl negalėtų būti plačiai taikoma. Taip pat kritikuotina, jog dabartiniai teisės aktai nenumato anonimizuotų duomenų saugojimo termino, o tai sudaro dingstis piktnaudžiauti. Kitos BDAR numatytos privatumo apsaugos garantijos abstraktesnio pobūdžio, bet taip pat reikšmingai prisideda prie privatumo apsaugos, nes veikia kaip standartizavimo šaltinis, kuriuo vadovaudamiesi bepiločių orlaivių rinkos dalyviai gali užsiimti kryptinga savireguliacija. Taigi sutikimas – pagrindinis ES duomenų apsaugos režimo ramstis, todėl BDAR, neskaitant kai kurių naudingų numatytų konkrečių privatumo apsaugos priemonių, privatumo apsauga, paremta *savarankiško privatumo valdymo* paradigma, būtų neveiksminga privatumo apsaugai bepiločių orlaivių naudojimo kontekste.

6. Savarankiškas privatumo valdymas, paremtas individo sutikimu, turi trūkumų. Duodami sutikimą tvarkyti duomenis, žmonės dažnai nesupranta realių savo pasirinkimo pasekmių arba jas supranta kiek iškreiptai dėl įgimto riboto racionalumo. Taip pat galima teigti, jog individai šių dienų rinkos sąlygomis neturi realios autonomijos priimti sprendimus, nes verslo modelių, pagal kuriuos būtų renkama mažiau duomenų, ekonomikoje tiesiog nėra, Žmonės taip pat neturi laiko skaityti privatumo politikų, tiksliai nenumato ilgalaikių duomenų tvarkymo ir derinimo tarpusavyje (agregavimo) pasekmių. Viena mokslinėje literatūroje siūlomų išeičių – paternalistinis reguliavimas, kuriuo iš esmės suvaržoma

individo pasirinkimo laisvė dėl jo paties gerovės. Paternalistinių nuostatų apstu įvairiuose šiuolaikiniuose teisės aktuose, tai būdinga ir BDAR, ir specialiajam bepiločių orlaivių reguliavimui. Disertacijos autoriaus siūlomas bepiločių orlaivių reguliavimo modelis taip pat paternalistinis. Jis paremtas ne sutikimu, o privalomo pobūdžio elgesio taisyklėmis, kurios nustatomos vadovaujantis formaliu reguliavimu. Pagrindinis dalykas, kuris daro šį reguliavimo modelį patrauklų, yra jo paprastumas. Jo taikymas leistų palengvinti teismų darbą, o per diskusijas dėl to, kaip turėtų būti reguliuojamas privatumas viešojoje erdvėje, įtrauktų plačiąją visuomenę. Disertacijos autoriaus vertinimu, siūlomas reguliavimas galėtų būti įgyvendintas per formalų reguliavimą, reguliavimą informuojant ir standartizavimą.

Daugiau disertacijos autoriaus vertinimų dėl problemų, kylančių naudojant bepiločius orlaivius, pateikta pačiame darbe.

REKOMENDACIJOS

1. ES reglamentai Nr. 2019/945 ir 2019/947 numato privalomus nuotolinio identifikavimo priedus daugeliui bepiločių orlaivių. Skrydžio identifikavimo duomenų transliavimas šiuo metu privalomas tik vietiniu būdu (radijo ryšiu), o tai apsunkina pažeidimų nustatymą, kai bepiločiais orlaiviais vykdoma slapta stebėsena. Išeitis galėtų būti identifikavimo duomenų transliavimas ne tik radijo ryšiu, bet ir internetu centrinei valdžios institucijai. Vis dėlto, kaip galima spręsti iš pastarųjų metų JAV patirties, šį pasiūlymą įgyvendinti šiuo metu būtų sudėtinga dėl nepakankamo nuotolinio identifikavimo technologijos išsivystymo. Taigi ES teisės aktų leidėjai į šį pasiūlymą turėtų atsižvelgti ateityje rengdami bepiločių orlaivių reglamentavimą, kai nuotolinio identifikavimo priedų technologija bus labiau išvystyta.

2. ES reglamentai Nr. 2019/945 ir 2019/947 numato reikalavimą saugoti įrašus apie vykdomą skrydį bepiločiu orlaiviu. Ši priemonė padėtų užtikrinti tam tikrą privatumo apsaugą, bet pagal dabartinį ES reguliavimą kaupiamų duomenų apimtis yra nepakankama, kad tai būtų veiksminga. Disertacijos autorius rekomenduoja kaupti daugiau asmens duomenų, kad iš jų būtų galima atkurti įvykdyto pažeidimo detales. Didinant kaupiamų duomenų apimtį, turėtų būti laikomasi šių sąlygų: 1) duomenys būtų tik bepilotyje orlaivyje, jie nebūtų pasiekiami internetu (juodosios dėžės), 2) duomenys tretiesiems asmenims būtų teikiami tik pagal teisėtą įgaliotos valdžios institucijos (teismo, ikiteisminio tyrimo pareigūno ar kt.) pareikalavimą, 3) duomenims būtų nustatytas konkretus ribotas saugojimo terminas.

3. ES reglamentai Nr. 2019/945 ir 2019/947 numato, jog bepiločiai orlaiviai, kurių svoris nesiekia 250 g, neprivalo turėti nuotolinio identifikavimo priedų. Ateityje daugiausia problemų dėl privatumo kels būtent nedideli bepiločiai orlaiviai, kurie be nuotolinio identifikavimo priedų nuotoliniu būdu bus neatpažįstami nukentėjusiems tretiesiems asmenims ar teisėsaugos institucijoms. Atsižvelgiant į tai, rekomenduotina keisti ES specialųjį bepiločių orlaivių reguliavimą, numatant, kad nuotolinius identifikavimo priedus būtų privaloma sieti ne tik su svoriu, bet ir analogiškai, kaip yra ES bepiločių orlaivių registracijos nuostatuose, su galimybe fiksuoti asmens duomenis. Tai, kad nuotoliniai identifikavimo priedai yra privalomi, galėtų būti siejama ir su registracijos reikalavimu (jei bepilotis registruotinas, jis turėtų turėti ir nuotolinio identifikavimo priedą).

4. ES reglamentai Nr. 2019/945 ir 2019/947 numato reikalavimą gaminti bepiločius orlaivius su žibintais. Dabartinis reguliavimas taiko išimtį bepiločiams orlaiviams, kurių svoris nesiekia 250 g, tačiau ir tokio svorio ar lengvesni bepiločiai orlaiviai gali pažeisti privatumą. Ateityje nedideliais bepiločiais orlaiviais privatumą pažeisti bus dar lengviau. Žibintai yra viena lengviausiai įgyvendinamų, pigiausių ir veiksmingiausių priemonių, galinčių apsaugoti privatumą. Todėl reikalavimas gaminti bepiločius orlaivius su žibintais turėtų būti taikomas visiems, kurie gali fiksuoti asmens duomenis, neatsižvelgiant į tai, ar skrydis vykdomas dienos ar nakties metu. Įgyvendinant šį pasiūlymą reikėtų nustatyti, kad bepiločių orlaivių šviesos šaltinis būtų tokio stiprumo, jog būtų matomas bent iš atstumo,

kuris galėtų veiksmingai apsaugoti privatumą ir atkreiptų pašalinių asmenų dėmesį netgi saulėtą dieną.

5. Kai asmens duomenys komerciniu tikslu renkami bepiločiu orlaiviu, pagal ES teisinį reguliavimą jo valdytojai privalo dar prieš skrydį gauti duomenų subjektų sutikimus. Iki atsirandant bepiločiams orlaiviams, sutikimas kaip privatumo apsaugos priemonė buvo dažniausiai naudojamas savarankiškam privatumo valdymui internete, tačiau šią priemonę pritaikyti bepiločiams orlaiviams sunku, nes jo valdytojui gauti sutikimą kiekvieną kartą prieš skrydį būtų sudėtinga. Dėl to, kad nėra pritaikytos teisinės bazės, ilgainiui tai gali tapti kliūtimi technologinei bepiločių orlaivių pažangai. Kaip išeitį disertacijos autorius rekomenduotų, kad teisėkūra ir teismai ateityje vadovautųsi paternalistinio pobūdžio ribų valdymo teorija, kuri paremta ne sutikimu, o privalomo pobūdžio elgesio taisyklėmis, nustatytomis vadovaujantis formaliu reguliavimu.

6. Daugelis šiais laikais prieinamų anonimizavimo technologijų turi imanentinių trūkumų, dėl kurių patikimai anonimizuoti duomenis šiuo metu neįmanoma. Nepaisant to, jog anonimišką informaciją jau įmanoma deanonimizuoti, teisės aktuose nėra numatyti tokių duomenų saugojimo terminai. Šia teisės aktų spraga gali pasinaudoti didžiųjų duomenų valdytojai sukeldami grėsmę privatumui per agregavimo, saugumo neužtikrinimo ir identifikavimo pažeidimus. Disertacijos autorius rekomenduotų teisės aktuose nustatyti anonimizuotų duomenų saugojimo terminą.

LITERATŪROS SĄRAŠAS

Teisės aktai

1. „1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, 13, 015 DD § (1995), http://data.europa.eu/eli/dir/1995/46/oj/lit.
2. „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (BDAR) (Tekstas svarbus EEE)“, 119 OJ L § (2016), http://data.europa.eu/eli/reg/2016/679/oj/lit.
3. „2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos“, OL L 152, 2019 m. birželio 11 d., 45–71.
4. „2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų“, OJ L 152, 2019 m. birželio 11 d., 1–40.
5. „Gegužės 3-iosios Konstitucija | *Magnus Ducatus Lithuaniae“,* žiūrėta 2022 m. gruodžio 21 d., http://www.mdl.projektas.vu.lt/thesaurus/kaupiamos-kolekcijos/rankrasciai/geguzes-3-konstitucija/.
6. „Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)“ (2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
7. „Remote Identification of Unmanned Aircraft Systems“, Notice of proposed rulemaking, Federal Aviation Administration (FAA), FAA-2019-1100, 84 FR 72438, 2019 m. gruodžio 31 d.
8. „Remote Identification of Unmanned Aircraft“, Final rule, Federal Aviation Administration (FAA), FAA-2019-1100, 86 FR 4390, 2021 m. sausio 15 d.
9. „Remote Identification of Unmanned Aircraft“, Final rule, Federal Aviation Administration (FAA), FAA-2019-1100, 86 FR 4390, 2021 m. sausio 15 d.
10. 14 United States Code of Federal Regulations 48.15(b).
11. 2001-03-14 LR Vyriausybės nutarimas „Dėl Lietuvos Respublikos vidaus reikalų ministerijos nuostatų patvirtinimo“ Nr. 291, *Valstybės žinios,* 2001-03-21, Nr. 24-794.
12. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) su paskutiniais pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB.
13. 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91.
14. 2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų, C/2019/1821, OJ L 152, 11.6.2019: 1–40 (Reglamentas (ES) 2019/945); 2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos, C/2019/3824, OJ L 152, 11.6.2019: 45–71 (Reglamentas (ES) 2019/947).
15. 49 United States Code 44809: Exception for limited recreational operations of unmanned aircraft.
16. Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022 (Federal Law Gazette I p. 968).

17. Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 6 des Gesetzes vom 7. November 2022 (BGBl. I S. 1982) geändert worden ist, § 12 Namensrecht.
18. *California Consumer Privacy Act of 2018* (CCPA); *California Civil Code* § 1798.100.
19. Council of Europe, „Convention for the Protection of Human Rights and Fundamental Freedoms", *Council of Europe Treaty Series 005* (Strasbourg: Council of Europe, 1950).
20. *FAA Reauthorization Act of 2018*.
21. Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems", FAA–2015–0150, *Federal Register,* 81, 124 (2016): 42064–42214.
22. Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems", FAA– 2015–0150, Federal Register, 81, 124 (2016): 42064–42214.
23. Federal Aviation Administration, „Operation of Small Unmanned Aircraft Systems Over People", Docket No.: FAA–2018–1087 § (2019), https://www.federalregister.gov/documents/2019/02/13/2019-00732/operation-of-small-unmanned-aircraft-systems-over-people.
24. ICAO Advisory Circular (AC) 101-1, (2020);
25. ICAO Advisory Circular (AC) 102-1, (2020);
26. ICAO Advisory Circular (AC) 102-23, (2020).
27. ICAO model UAS regulations part 101 and 102, (2020);
28. ICAO model UAS regulations part 149, (2020);
29. JAV Federalinių teisės aktų kodeksas
30. JAV Konstitucijos ketvirtoji pataisa
31. JAV Konstitucijos pirmoji pataisa
32. Lietuvos Tarybų Socialistinės Respublikos Konstitucija (Pagrindinis įstatymas), LR Aukščiausioji Taryba, *Vyriausybės žinios,* 1978-01-01, 11–130.
33. *Lietuvos Tarybų Socialistinės Respublikos Konstitucija* (Pagrindinis Įstatymas). Vilnius: Lietuvos Liaudies Seimas, 1940-08-25.
34. Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1922, „LR Konstitucija – 1922 m. Lietuvos Valstybės Konstitucija", žiūrėta 2022 m. gruodžio 21 d., https://www.lrk.lt/lietuvos-konstitucijos-istorija/202-1922-m-lietuvos-valstybes-konstitucija.
35. Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1928, „1928_m._Lietuvos_Valstybės_Konstitucija.IH2105.pdf", žiūrėta 2022 m. gruodžio 21 d., http://www.xn--altiniai-4wb.info/files/istorija/IH00/1928_m._Lietuvos_Valstyb%C4%97s_Konstitucija.IH2105.pdf.
36. Lietuvos Valstybės Konstitucija, *Vyriausybės žinios,* 1938, „Iš 1938 m. Lietuvos Konstitucijos", http://www.xn--altiniai-4wb.info/files/istorija/IH00/I%C5%A1_1938_Lietuvos_Konstitucijos.IH2106.pdf.
37. LR administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas. LR administracinių nusižengimų kodeksas, suvestinė (2022-11-01–2022-12-31) redakcija, LR Seimas, XII-1869, TAR, 2015-07-10, Nr. 11216.
38. LR autorių teisių ir gretutinių teisių įstatymas, VIII-1185, *Valstybės žinios,* 1999-06-09, Nr. 50-1598.
39. LR baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas, suvestinė (2022-11-01–2022-12-31) redakcija, LR Seimas, VIII-1968, *Valstybės žinios,* 2000-10-25, Nr. 89-2741, XXIV skyrius, 167–168 straipsniai.
40. LR civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Civilinis kodeksas, VIII-1864, *Valstybės žinios,* 2000-09-06, Nr. 74-2262.
41. LR civilinio proceso kodeksas (suvestinė redakcija nuo 2020-07-09), *Žin.* (2002-04-06, Nr. 36-1340).
42. LR elektroninių ryšių įstatymas (suvestinė redakcija nuo 2020-01-17), *Žin.* (2004, Nr. 69-2382).
43. LR Konstitucija, 1992 m. lapkričio 2 d., *Lietuvos aidas,* 1992, 220 (1992-11-10); Valstybės žinios, 1992, 33-1014 (1992-11-30).
44. LR susirinkimų įstatymas, *Valstybės žinios,* 136, 6956 (2012), 4 straipsnio 1 dalis.

45. LR triukšmo valdymo įstatymas, *Valstybės žinios,* 164, 5971 (2004), 6 straipsnio 1 punktas.
46. Prancūzijos 1791 m. rugsėjo 3 d. Konstitucija.
47. SESAR Joint Undertaking, „European ATM master plan“ (Publications Office of the European Union, 2020).
48. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 11. Juli 2022 (BGBl. I S. 1082) geändert worden ist, § 185 Beleidigung.
49. The Privacy Act of 1974, pakeistas 5 U.S.C. § 552a.
50. U.S. Reauthorization Act of (2018).
51. UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, 171, 17 straipsnis, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.174848.
52. Viešosios įstaigos Transporto kompetencijų agentūros direktoriaus 2021 m. lapkričio 5 d. įsakymas Nr. 2-134 „Dėl leidimų vykdyti specialiosios kategorijos skrydžius naudojant bepiločio orlaivio sistemą išdavimo tvarkos aprašo patvirtininimo“ (Suvestinė redakcija nuo 2023-12-02).
53. Visuomenės informavimo įstatymas (suvestinė redakcija nuo 2023-05-01), Žin. (1996, Nr. 71-1706)

Oficialios rekomendacijos, gairės

1. „2009 m. birželio 18 d. Europos Parlamento ir Tarybos direktyva 2009/48/EB dėl žaislų saugos“, OJ L 170, 2009 m. birželio 30 d., 1–37.
2. „Aircraft Registration | Federal Aviation Administration“, žiūrėta 2022 m. gruodžio 16 d., https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/ua.
3. „Article 29 Working Party | European Data Protection Board“, žiūrėta 2022 m. lapkričio 14 d., https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en.
4. „Civil Drones (Unmanned Aircraft)“, EASA, žiūrėta 2020 m. rugsėjo 14 d., https://www.easa.europa.eu/domains/civil-drones-rpas.
5. „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“, Valstybinės duomenų apsaugos inspekcijos direktorius, 1T-35 (1.12.E), TAR, 2019-03-14, Nr. 4104.
6. „Fact Sheet – Small Unmanned Aircraft Regulations (Part 107)“, žiūrėta 2020 m. liepos 28 d., https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516.
7. „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, Europos duomenų apsaugos valdyba, 2020-05-04.
8. „Guidelines on transparency under Regulation 2016/679“, Article 29 data protection working party, 17/EN, WP260 (2018).
9. „JARUS guidelines on Specific Operations Risk Assessment (SORA)“, No. JAR-DEL-WG6-D.04, 2019-01-30.
10. „JARUS Recommendations for Unmanned Aircraft Systems (UAS) Category A & Category B Operations“, 2019-07-11, http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_14_ops_cat_a_b_edition1.0.pdf.
11. „Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį“, 29 straipsnio duomenų apsaugos darbo grupė, 844/14/LT, WP 217 (2014).
12. „Opinion 05/2014 on Anonymisation Techniques“, Article 29 data protection working party, 0829/14/EN, WP216.
13. „Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų“, 29 straipsnio duomenų apsaugos grupė, WP 248, 1-oji peržiūrėta versija, 17/LT (2017).
14. „Rekomendacija dėl vaizdo duomenų tvarkymo daugiabučiuose ir privačiuose gyvenamuosiuose namuose“, VDAI, (2019).

15. „Rekomendacija smulkiajam ir vidutiniam verslui dėl Bendrojo duomenų apsaugos reglamento taikymo“, VDAI, 2018-09-05, https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacijos_smulkiajam%20ir%20vidutiniam%20verslui%20del%20BDAR%20taikymo%202018-09-05.pdf.
16. „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, VDAI, 3 versija (2020).
17. „Voluntary Best Practices for UAS Privacy, Transparency, and Accountability“ (National Telecommunications and Information Administration, 2016).
18. Council of Europe Human Rights Commissioner's Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, CommDH (2016)20, 2016;
19. Council of Europe Parliamentary Assembly resolution on Terrorist attacks in Paris: together for a democratic response, 2015.
20. European Union Aviation Safety Agency, „Opinion No 05/2019 – Standard scenarios for UAS operations in the 'specific' category“, (2019).
21. Federal Aviation Administration, „Advisory Circular No. 107-2“ (AC 107-2), (2016): 6–4, www.faa.gov/documentlibrary/media/advisory_circular/ac_107-2.pdf.
22. Federal Aviation Administration, „Remote Pilot – Small Unmanned Aircraft Systems (Certification and Recurrent Knowledge Testing) Airman Certification Standards“, Flight Standards ServiceWashington, DC 20591, 2018; www.faa.gov/training_testing/testing/acs/media/uas_acs.pdf, „Policy Document Library“, template, žiūrėta 2020 m. spalio 14 d., https://www.faa.gov/uas/resources/policy_library/#107.
23. ICAO Advisory Circular (AC) 101-1, (2020);
24. ICAO Advisory Circular (AC) 102-1, (2020);
25. ICAO Advisory Circular (AC) 102-23, (2020);
26. ICAO model UAS regulations part 101 and 102, (2020);
27. ICAO model UAS regulations part 149, (2020);
28. JARUS UAS Operational Categorization (2019).
29. Joint Authorities for Rulemaking of Unmanned Systems, „Recommendations on the use of Controller Pilot Data Link Communications (CPDLC) in the RPAS communications context“, 2016 m. vasario 6 d.;
30. Joint Authorities for Rulemaking of Unmanned Systems, „Required C2 Performance (RLP) concept“, 2016 m. sausio 5 d.
31. Joint Authorities for Rulemaking of Unmanned Systems, „RPAS C2 link Required Communication Performance (C2 link RCP) concept“, 2014 m. spalio 10 d.;

Teismų praktika

1. „Antović and Mirković v. Montenegro“, No. 70838/13 (ECtHR 2017 m. lapkričio 28 d.).
2. „B. v. France“, No. 57/1990/248/319 (European Court of Human Rights 1992 m. sausio 24 d.).
3. „Bărbulescu v. Romania”, No. 61496/08 (ECtHR [GC] 2017 m. rugsėjo 5 d.);
4. „Bellet v. France“, 4 December 1995, Series A no. 333-B.
5. „Big Brother Watch and Others v. the United Kingdom“, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 2021 m. gegužės 25 d.).
6. „Big Brother Watch and Others v. the United Kingdom“, op. cit. (ECtHR 2018 m. rugsėjo 13 d.).
7. „Boyd v. United States“, 116 U.S. 616 (1886).
8. „California v. Greenwood“, 486 U.S. 35 (1988) .
9. „Case C-212/13 on CCTV“. http://curia.europa.eu/juris/document/document.jsf?text=95%252F46%252FEC&docid=160561&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=300923#ctx1.
10. „Centrum För Rättvisa v. Sweden“, No. 35252/08 (ECtHR [GC] 2021 m. gegužės 25 d.).
11. „Costello-Roberts v. The United Kingdom“, 89/1991/341/414, Council of Europe: European Court of Human Rights, 23 February 1993.
12. „Cox Broadcasting Corp. v. Cohn“, 420 U.S. 469 (1975).

13. „Fazliyski v. Bulgaria“, no. 40908/05, 16 April 2013.
14. „Felix c. O'Connell“, Trib. civ. S[e]ine, June 16, 1858, 4 A.P.I.A.L. 250 (1858).
15. „Herbecq and the Association „Ligue Des Droits De L'homme“ v. Belgium (dec.)”, No. 32200/96, 32201/96 (EComHR 1998 m. sausio 14 d.).
16. „Hustler Magazine, Inc. v. Falwell“, 485 U.S. 46 (1988).
17. „Katz v. United States“, No. 389 U.S. 347 (Supreme Court of the United States 1967 m. gruodžio 18 d.).
18. „Köpke v. Germany (dec.)”, No. 420/07 (ECtHR 2010 m. spalio 5 d.);
19. „Lawrence v. Texas“, 539 U.S. 558 (2003).
20. „López Ribalda and Others v. Spain”, No. 1874/13, 8567/13 (ECtHR [GC] 2019 m. spalio 17 d.).
21. „Midler v. Ford Motor Co.“, 849 F.2d 460 (9th Cir. 1988).
22. „Niemietz v. Germany”, No. 13710/88 (ECtHR 1992 m. gruodžio 16 d.).
23. „Niemietz v. Germany“, No. 13710/88 (ECtHR 1992 m. gruodžio 16 d.).
24. „Nunes Dias v. Portugal“ (dec.), nos. 2672/03 and 69829/01, ECHR 2003-IV.
25. „P. G. and J. H. V. the United Kingdom”, No. 44787/98 (ECtHR 2001 m. rugsėjo 25 d.);
26. „Peck v. the United Kingdom“, No. 44647/98 (ECtHR 2003 m. sausio 28 d.).
27. „Perry v. the United Kingdom”, No. 63737/00 (ECtHR 2003 m. liepos 17 d.);
28. „S. A. Multimania Prod. c. Madame L.“, No. 859, CA Versailles, 12eme ch., June 8, 2000; S.A. SPPI c. Societh Fox Media, No. R6: 01/04400, T.G.I. Paris, 3eme ch., May 29, 2002.
29. „Schmerber v. California“, 384 U.S. 757 (1966).
30. „Sergent c. Defonds“, Trib. civ. Seine, Nov. 11, 1859, 6 Annales de la Propriete Industrielle Artistique et Litteraire [A.P.I.A.L.] 168 (1860).
31. „Söderman v. Sweden”, No. 5786/08 (ECtHR [GC] 2013 m. lapkričio 12 d.);
32. „Thompson v. Johnson County Community College”, 930 F. Supp. 501 (D. Kan. 1996)
33. „United States v. Scott“, 437 U.S. 82 (1978).
34. „United States v. Stevens”, 559 U.S. 460 (2010)“, *Justia Law,* žiūrėta 2022 m. lapkričio 7 d., https://supreme.justia.com/cases/federal/us/559/460/.
35. „Vanna White v. Samsung Elecs. Am.“, Inc., 989 F. 2d 1512 (9th Cir. 1993).
36. „Von Hannover v. Germany (no. 2)”, No. 40660/08, 60641/08 (ECtHR [GC] 2012 m. vasario 7 d.).
37. „Vukota-Bojic v. Switzerland”, No. 61838/10 (ECtHR 2016 m. spalio 18 d.).
38. „Weber and Saravia v. Germany (dec.)“, No. 54934/00 (ECtHR 2006 m. birželio 29 d.).
39. „Whalen v. Roe“, No. 429 U.S. 589 (Supreme Court of the United States 1977 m. vasario 22 d.).
40. „Zubac v. Croatia [GC]“, no. 40160/12, 5 April 2018.
41. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado, No. Joined cases C-468/10 and C-469/10 (ECJ 2011 m. lapkričio 24 d.).
42. Case C-212/13 on CCTV http://curia.europa.eu/juris/document/document.jsf?text=95%252F46%252FEC&docid=160561&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=300923#ctx1.
43. Dumas c. Liébert, CA Paris, 1867 m. gegužės 25 d., 13 A.P.I.A.L. (1867).
44. Eden c. Whistler, Cass. civ., Mar. 14, 1900, D.P. (1900);
45. Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, No. Case C-131/12 (ECJ 2014 m. gegužės 13 d.);
46. Herbecq and the Association „Ligue Des Droits De L'homme v. Belgium (dec.)“.
47. Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others, ECLI:EU:C:2020:791, Grand Chamber Judgment, at 136 (Ct. Just. Eur. Union Oct. 6, 2020), at http://curia.europa.eu/juris/document/ document.jsf?text¼&docid¼232084&pageIndex¼0&doclang¼EN&mode¼lst&dir¼&occ¼first&part¼ 1&cid¼6166350.

48. LAT 2001 m. balandžio 18 d. sprendimas civilinėje byloje Nr. 3K-3-461.
49. LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.
50. LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.
51. LAT 2003 m. vasario 24 d. sprendimas civilinėje byloje Nr. 3K-3-294/2003.
52. LAT 2008 m. rugsėjo 23 d. nutartį civilinėje byloje Nr. 3K-3-394/2008.
53. LAT 2008 m. rugsėjo 23 d. nutartis civilinėje byloje Nr. 3K-3-394/2008.
54. LAT Baudžiamųjų bylų skyriaus 2015 m. birželio 1 d. nutartis baudžiamojoje byloje Nr. 2K-P-94-895/2015. *Teismų praktika,* 43, (2015): 476–465.
55. LAT Baudžiamųjų bylų skyriaus 2017 m. vasario 21 d. nutartis baudžiamojoje byloje Nr. 2K-57-696/2017, *Teismų praktika* 47, (2017): 540–554.
56. LAT Civilinių bylų skyriaus 2002 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 3K-3-1406.
57. LAT Civilinių bylų skyriaus 2004 m. gegužės 3 d. nutartis civilinėje byloje Nr. 3K-3-289.
58. LAT Civilinių bylų skyriaus 2004 m. gegužės 3 d. nutartis civilinėje byloje Nr. 3K-3-289.
59. LAT Civilinių bylų skyriaus 2004 m. vasario 9 d. nutartis civilinėje byloje Nr. 3K-3-91.
60. LAT Civilinių bylų skyriaus 2004 m. vasario 9 d. nutartis civilinėje byloje Nr. 3K-3-91.
61. LAT Civilinių bylų skyriaus 2008 m. rugsėjo 23 d. nutartis civilinėje byloje Nr. 3K-3-394/2008.
62. LAT Civilinių bylų skyriaus 2008 m. rugsėjo 23 d. nutartis civilinėje byloje Nr. 3K-3-394/2008.
63. LAT Civilinių bylų skyriaus 2009 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-26/2009.
64. LAT Civilinių bylų skyriaus 2009 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-26/2009.
65. LAT Civilinių bylų skyriaus 2017 m. gruodžio 27 d. nutartis civilinėje byloje Nr. e3K-3-472-916/2017.
66. LAT Civilinių bylų skyriaus 2020 m. spalio 28 d. nutartis civilinėje byloje Nr. e3K-3-278-403/2020. *Teismų praktika* 54 (2020): 11–24.
67. LAT Civilinių bylų skyriaus 2020 m. spalio 28 d. nutartis civilinėje byloje Nr. e3K-3-278-403/2020, *Teismų praktika* 54 (2020): 11–24.
68. Le Figaro c. Chaperon, CA Paris, 4e ch., Dec. 2, 1897, 45 A.P.I.A.L. 61 (1899).
69. Moitessier c. Féral, Tribunal civil de la Seine, 1877 m. gruodžio 5 d., 23 A.P.I.A.L. (1878);
70. Patrick Breyer v. Bundesrepublik Deutschland, No. Case C-582/14 (ECJ 2016 m. spalio 19 d.);
71. Soeur Melanie c. Foug6re, Ord. de R66r6, Apr. 11, 1855, 6 A.P.I.A.L. 167 (1860).
72. Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme“, No. Case C-13/16 (ECJ 2017 m. gegužės 4 d.).
73. Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme“.

Mokslinė literatūra

1. Acquisti ir J. Grossklags, „Privacy and rationality in individual decision making“, *IEEE Security & Privacy* 3, 1 (2005): 26–33, https://doi.org/10.1109/MSP.2005.22.
2. Bakanas ir kiti, *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys* (Vilnius: Justitia, 2002), 60.
3. Adam Rothstein, *Drone,* Object Lessons (London: Bloomsbury Academic, 2015).
4. Ahmad Javaid ir kt., „Cyber security threat analysis and modeling of an unmanned aerial vehicle system“, 2012, p. 586, https://doi.org/10.1109/THS.2012.6459914.
5. Alan F. Westin, „Privacy and freedom“, *Washington and Lee Law Review* 25, 1 (1968).
6. Aleecia M. McDonald ir Lorrie Faith Cranor, „The cost of reading privacy policies“, *Isjlp* 4 (2008).
7. Alessandro Acquisti ir Jens Grossklags, „Privacy and rationality“, *Privacy and Technologies of Identity* (Springer, 2006), 15–29.
8. Alessandro Acquisti ir kt., „What can behavioral economics teach us about privacy?“, *Digital privacy* (Auerbach Publications, 2007).
9. Alfonsas Vaišvila, *Teisės teorija* (Vilnius: Justitia, 2005).
10. Alfonsas Vaišvila, *Teisinis personalizmas: teorija ir metodas:(teisės sugrąžinimo visuomenei ideologija)* (Vilnius: Justitia, 2011).

11. Alphonse Barthélemy Martin Boistel, *Cours de philosophie du droit: professé à la Faculté de droit de Paris,* t. 1 (A. Fontemoing, 1899).
12. André Bertrand, *Droit à la vie privée et droit à l'image* (Lexis Nexis, 1999).
13. Ann Christiano ir Annie Neimand, „Stop raising awareness already", *Stanford Social Innovation Review* 15, 2 (2017): 34–41.
14. Anna Pastore, „Consent Notices and Cognitive Cost after the GDPR : An Experimental Study" (masterThesis, 2020), https://repositorio.ucp.pt/handle/10400.14/31285.
15. Anne Millbrooke, "Aviation History" (Englewood: Jeppesen, 2006), 1–20.
16. Antoinette Rouvroy ir Yves Poullet, „The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy", Reinventing data protection? (Springer, 2009), 45–76; Orla Lynskey, *The foundations of EU data protection law* (Oxford University Press, 2015).
17. Anupam Chander, Margot E. Kaminski ir William McGeveran, „Catalyzing Privacy Law", Minnesota Law Review 105, 4 (2021): 1733–1802.
18. Arie Rip, „De facto Governance of Nanotechnologies", *Futures of Science and Technology in Society,* (Wiesbaden: Springer Fachmedien Wiesbaden, 2018), 75–96, https://doi.org/10.1007/978-3-658-21754-9_5.
19. Arjaan Wit ir Henk A. Wilke, „The presentation of rewards and punishments in a simulated social dilemma.", *Social Behaviour,* (1990).
20. Ashley Thomas, „NO PLACE TO HIDE: Privacy Implications of Geolocation Tracking and Geofencing", *Scitech Lawyer* 16, 2 (2020): 20–23.
21. Aurelija Pūraitė ir Neringa Šilinskė, „Privacy Protection in the New Eu Regulations on the Use of Unmanned Aerial Systems", *Public Security and Public Order,* 24 (2020).
22. Aurelija Pūraitė, Daiva Bereikienė ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania", *Baltic Journal of Law & Politics* 10, 2 (2017): 107–132.
23. Aurimas Šidlauskas, „Video Surveillance and the GDPR", 2019.
24. Bart van der Sloot, Dennis Broeders ir Erik Schrijvers, *Exploring the boundaries of Big Data* (Amsterdam: University Press Amsterdam, 2016).
25. Benjamin Wittes ir Emma Kohse, *The privacy paradox II: Measuring the privacy benefits of privacy threats* (Center for Technology Innovation at Brookings, 2017);
26. Carl Martin Allwood ir Tomas Kalén, „Evaluating and improving the usability of a user manual", *Behaviour & Information Technology* 16, 1 (1997): 43–57.
27. Christine Haynes, *Lost Illusions: The Politics of Publishing in Nineteenth-Century France* (Harvard University Press, 2010).
28. Christoph Bösch, „An Efficient Privacy-Preserving Outsourced Geofencing Service Using Bloom Filter", *2018 IEEE Vehicular Networking Conference (VNC)* (IEEE, 2018): 1–8.
29. Christopher McCusker ir Peter J. Carnevale, „Framing in resource dilemmas: Loss aversion and the moderating effects of sanctions", *Organizational Behavior and Human Decision Processes* 61, 2 (1995): 190–201.
30. Claudia Quelle, „Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection", *Privacy and Identity Management. Facing up to Next Steps,* sud. Anja Lehmann ir kt., t. 498, IFIP Advances in Information and Communication Technology (Cham: Springer International Publishing, 2016), 140–163, https://doi.org/10.1007/978-3-319-55783-0_11.
31. Claudia Quelle, „Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection", *Privacy and Identity Management. Facing up to Next Steps,* sud. Anja Lehmann ir kt., t. 498, IFIP Advances in Information and Communication Technology (Cham: Springer International Publishing, 2016): 140–63, https://doi.org/10.1007/978-3-319-55783-0_11.
32. Dan Ariely ir Simon Jones, *Predictably irrational* (HarperCollins New York, 2008).
33. Dan M. Kahan, „A risky science communication environment for vaccines", *Science* 342, 6154 (2013).

34. Daniel Eek ir kt., „Spill-over effects of intermittent costs for defection in social dilemmas“, *European Journal of Social Psychology* 32, 6 (2002): 801–13.
35. Daniel J. Solove, „A Taxonomy of Privacy“, *University of Pennsylvania Law Review* 154, 3 (2006): 477–564;
36. Daniel J. Solove, „Conceptualizing Privacy“, *California Law Review* 90, 4 (2002): 1087–1156;
37. Daniel J. Solove, „I've got nothing to hide and other misunderstandings of privacy“, *San Diego L. Rev.* 44 (2007): 745;
38. Daniel J. Solove, „Introduction: Privacy self-management and the consent dilemma“, Harv. L. Rev. 126 (2012).
39. Daniel J. Solove, „Understanding privacy“, 2008;
40. Daniel Le Métayer ir Julien Le Clainche, „From the protection of data to the protection of individuals: extending the application of non-discrimination principles“, *European Data Protection: In Good Health?* (Springer, 2012), 315–329.
41. Deividas Kiršys, „Ar bepiločio orlaivio skrydžio vykdymas žemės sklypo oro erdvėje nepažeidžia to žemės sklypo savininko nuosavybės teisės?“ (Vytautas Magnus University, 2016).
42. Dennis D. Hirsch „That's unfair-or is it: Big data, discrimination and the FTC's unfairness authority“, Ky, LJ 103 (2014): 345.
43. Des Butler, „The Dawn of the Age of the Drones: An Australian Privacy Law Perspective“, *University of New South Wales Law Journal* 37, 2 (2014): 434–470.
44. Egidijus Baranauskas ir kt., „Civilinė teisė. Bendroji dalis: vadovėlis aukštųjų mokyklų studentams“, (Vilnius: Mykolo Romerio universitetas, 2007), 48.
45. Eleonora Bassi ir kt., „The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management“, *Minds and Machines* 29, 4 (2019): 579–601.
46. Elinor Ostrom, James Walker ir Roy Gardner, „Covenants with and without a sword: Self-governance is possible“, *American political science Review* 86, 2 (1992): 404–417.
47. Emile Beaussire, *Les principes du droit* (Alcan, 1888).
48. Emile Beaussire, *Les principes du droit* (Alcan, 1888).
49. Emma C. Bullock, „A Normatively Neutral Definition of Paternalism“, *The Philosophical Quarterly* 65, 258 (2015 m. sausio 1 d.): 1–21, https://doi.org/10.1093/pq/pqu056. David Archard, „Paternalism defined“, Analysis 50, 1 (1990): 36–42.
50. Ernst Fehr ir Armin Falk „Psychological Foundations of Incentives“, *European Economic Review* 46, 4–5 (2002): 687–724.
51. Europäische Kommission ir Europäische Kommission, sud., *Flightpath 2050: Europe's Vision for Aviation; Maintaining Global Leadership and Serving Society's Needs; Report of the High-Level Group on Aviation Research,* Policy / European Commission (Luxembourg: Publ. Off. of the Europ. Union, 2011).
52. Ferdinand Schoeman, „Gossip and privacy“, 1994.
53. Fred Samland ir kt., „AR.Drone: Security threat analysis and exemplary attack to track persons“, *Proceedings of SPIE – The International Society for Optical Engineering* 8301 (2012 m. sausio 22 d.).
54. Gary E. Marchant, Braden R. Allenby ir Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Dordrecht Heidelberg London New York: Springer Science & Business Media, 2011).
55. Gary S. Becker, „Crime and punishment: An economic approach“, *The economic dimensions of crime* (Springer, 1968), 13–68;
56. Gediminas Bučiūnas, „Vaizdo registratoriai ir asmens privatumas“, *Mokslo taikomieji tyrimai Lietuvos kolegijose* 1, 11 (2015): 64–68; Gediminas Bučiūnas, „Sekimas ir asmens privatumas: kur riba?“ (Vilnius: Mykolo Romerio universitetas, 2010).
57. George Orwell ir A. M. Heath, *Animal farm and 1984* (Houghton Mifflin Harcourt, 2003).

58. Gerald Dworkin, *The theory and practice of autonomy* (Cambridge University Press, 1988); Gerald Dworkin, „Defining Paternalism“, *New Perspectives on Paternalism and Health Care,* sud. Thomas Schramme, Library of Ethics and Applied Philosophy (Cham: Springer International Publishing, 2015), 17–29, https://doi.org/10.1007/978-3-319-17960-5_2.
59. Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation“, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): 172.
60. Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation“, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): [i]-177.
61. Gerd Kleinheyer, „Dieter Leuze, Die Entwicklung des Persönlichkeitsrechts im 19. Jh. Zugleich ein Beitrag zum Verhältnis allgem. Persönlichkeitsrecht–Rechtsfähigkeit“, *Zeitschrift der Savigny-Stiftung für Rechtsgeschichte: Germanistische Abteilung* 81, 1 (1964).
62. Giuseppe Contissa ir kt., „Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence“, *SSRN Electronic Journal,* 2018 m. sausio 1 d., https://doi.org/10.2139/ssrn.3208596.
63. Giuseppe D'Acquisto ir kt., *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics,* 2015, https://doi.org/10.2824/641480.
64. Helen Nissenbaum, „Privacy as Contextual Integrity Symposium – Technology, Values, and the Justice System“, *Washington Law Review* 79, 1 (2004).
65. Helen Nissenbaum, „Protecting Privacy in an Information Age: The Problem of Privacy in Public“, *Law and Philosophy* 17, 5/6 (199): 559–596.
66. Helen Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life* (Stanford University Press, 2009).
67. Hwai-Jung Hsu ir Kuan-Ta Chen, „Face recognition on drones: Issues and limitations“, *Proceedings of the first workshop on micro aerial vehicle networks, systems, and applications for civilian use* (2015).
68. Yaxing Yao ir kt., „Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders“, *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (ACM, 2017), 6785.
69. Yola Georgiadou, Rolf A. de By ir Ourania Kounadi, „Location Privacy in the Wake of the GDPR“, *ISPRS International Journal of Geo-Information* 8, 3 (2019): 157, https://doi.org/10.3390/ijgi8030157.
70. Jacques Pelkmans ir Andrea Renda, „Does EU Regulation Hinder or Stimulate Innovation?“, CEPS special report (Brussels: Centre for European Policy Studies, 2014).
71. James Q. Whitman, „Enforcing Civility and Respect: Three Societies“, *Yale Law Journal* 109, 6 (2000): 1279–1398.
72. James Q. Whitman, „Origins of Law and the State: Supervision of Violence, Mutilation of Bodies, or Setting of Prices, At the“, *Chi.-Kent L. Rev.* 71 (1995).
73. James Q. Whitman, „The Two Western Cultures of Privacy: Dignity versus Liberty“, *Yale Law Journal 113,* 6 (2004): 1151–1222.
74. Jane Andrew ir Max Baker, „The general data protection regulation in the age of surveillance capitalism“, *Journal of Business Ethics* 168, 3 (2021): 565–578.
75. Jennifer L. Jacquet ir Daniel Pauly, „The rise of seafood awareness campaigns in an era of collapsing fisheries“, *Marine Policy* 31, 3 (2007): 308–13.
76. Jens Mathias Bohli ir kt., „PrivLoc: preventing location tracking in geofencing services“, *International Conference on Trust and Trustworthy Computing* (Springer, 2014), 143–60.
77. Jeremy Bentham, *Panopticon Or the Inspection House* (T. Payne, 1791).
78. Jeremy Packer, „Epistemology Not Ideology OR Why We Need New Germans“, *Communication and Critical/Cultural Studies* 10, 2–3 (2013 m. rugsėjo mėn.).

79. Jérôme Pétion, „Suite du discourse sur la liberté de la Presse“, 16 Courier de Provence 199 (1791).
80. Jill R. Applebaum, „The Visual Artists Rights Act of 1990: An Analysis Based on the French Droit Moral Notes and Comments“, *American University Journal of International Law and Policy* 8, 1 (1993): 183–224.
81. Joel R. Reidenberg, „Privacy in Public“, *University of Miami Law Review* 69, 1 (2014): 141–160.
82. Johannes Heurix ir kt., „A Taxonomy for Privacy Enhancing Technologies“, *Computers & Security* 53, (2015): 1–17, https://doi.org/10.1016/j.cose.2015.05.002.
83. John F. Keane ir Stephen S. Carr, „A brief history of early unmanned aircraft“. *Johns Hopkins APL Technical Digest* 32, 3 (2013): 558–571.
84. Jonathan B. Clark, „Overview of Balloon Flights and Their Biomedical Impact on Human Spaceflight“, *Handbook of Bioastronautics,* (2021), 839–856.
85. Jonathan P. West ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues“, *Public Administration Review* 76, 4 (2016): 649–659.
86. Jonathon W. Penney, „Understanding Chilling Effects“, *Minnesota Law Review* 106, 3 (2022).
87. Josef Kohler, *Das Autorrecht, eine zivilistische Abhandlung: zugleich ein Beitrag zur Lehre vom Eigenthum, vom Miteigenthum, vom Rechtsgeschäft und vom Individualrecht,* t. 6 (G. Fischer, 1880).
88. Judith Wagner DeCew, *In pursuit of privacy: Law, ethics, and the rise of technology* (Cornell University Press, 1997).
89. Julia Daisy Fraustino ir Liang Ma, „CDC's Use of Social Media and Humor in a Risk Campaign – „Preparedness 101: Zombie Apocalypse“, *Journal of Applied Communication Research* 43, 2 (2015): 222–241, https://doi.org/10.1080/00909882.2015.1019544.
90. Julian Wagner ir Alexander Benecke, „National Legislation within the Framework of the GDPR“, *European Data Protection Law Review* (EDPL) 2, 3 (2016): 353–61.
91. Juozapas Vytas Urbonas, „Spaudos laisvė ir jos įtaka kuriant pilietinę visuomenę“, *Tiltai: humanitariniai ir socialiniai mokslai,* 1 (2005): 115–22.
92. Kalle Grill, „Anti-paternalism and public health policy“ (KTH, 2009). Gerald Dworkin, „Defining Paternalism“, *New Perspectives on Paternalism and Health Care,* sud. Thomas Schramme, Library of Ethics and Applied Philosophy (Cham: Springer International Publishing, 2015), 17–29, https://doi.org/10.1007/978-3-319-17960-5_2.
93. Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu“ (Vilnius: Mykolo Romerio universitetas, 2019, 70-71.
94. Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu“ (Vilnius: Mykolo Romerio universitetas, 2019).
95. Kearston L. Wesner, „Is the Grass Greener on the Other Side of the Geofence: The First Amendment and Privacy Implications of Unauthorized Smartphone Messages“, *Case Western Reserve Journal of Law, Technology and the Internet* 10 (2019): [iii]-23;
96. Kelly A. Gates, „Our biometric future“, *Our Biometric Future* (New York University Press, 2011).
97. Kevin D. Haggerty, Richard V. Ericson, „The Surveillant Assemblage“, *British Journal of Sociology* 51, 4 (2000 m. gruodžio 1 d.).
98. Klaus Schwab, *The fourth industrial revolution* (New York: Crown Business, 2017), 1–5.
99. Laura Brandimarte, Alessandro Acquisti ir George Loewenstein, „Misplaced confidences: Privacy and the control paradox“, *Social psychological and personality science* 4, 3 (2013): 340–347.
100. Laurynas Pakštaitis, „Senovės romėnų baudžiamosios teisės bruožai“, Research Journal *Public security and public order* 30 (2022).
101. Leysia Palen ir Paul Dourish, „Unpacking *Privacy* for a Networked World“, Proceedings of the SIGCHI conference on Human factors in computing systems (2003).

102. Lyria Bennett Moses, „Agents of Change: How the Law 'Copes' with Technological Change", *Griffith Law Review* 20, 4 (2011): 763–794, https://doi.org/10.1080/10383441.2011.10854720.
103. Louis Brandeis ir Samuel Warren, „The Right to Privacy'", *Harvard Law Review* 4. (1890): 193–220.
104. Luke A. Stewart, „The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review", *Information Technology & Innovation Foundation,* (2010).
105. Mamoona Asghar ir kt., „Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective", *IEEE Access* 7 (2019 m. rugpjūčio 9 d.): 111709–111726, https://doi.org/10.1109/ACCESS.2019.2934226.
106. Margherita Bonetto ir kt., „Privacy in mini-drone based video surveillance", *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition* (FG), 4 (IEEE, 2015), 1–6.
107. Margot E. Kaminski, „Regulating Real-World Surveillance", *Washington Law Review* 90, 3 (2015): 1113–1166.
108. Maryam Mazaheri ir kt., „Market-Based Instruments and Sustainable Innovation: A Systematic Literature Review and Critique", *Journal of Cleaner Production* 373 (2022): 133947, https://doi.org/10.1016/j.jclepro.2022.133947.
109. Mariana Cunha, Ricardo Mendes ir João P. Vilela, „Clustering Geo-Indistinguishability for Privacy of Continuous Location Traces", *2019 4th International Conference on Computing, Communications and Security (ICCCS)* (IEEE, 2019): 1–8.
110. Mark Andrejevic ir Kelly Gates, „Big Data Surveillance: Introduction", *Surveillance & Society* 12, 2 (2014 m. gegužės 9 d.), 185–196, https://doi.org/10.24908/ss.v12i2.5242.
111. Mark Van Vugt ir David De Cremer, „Leadership in social dilemmas: The effects of group identification on collective actions to provide public goods.", *Journal of personality and social psychology* 76, 4 (1999).
112. Melville B. Nimmer, „The right of publicity", *Law and Contemporary problems* 19, 2 (1954): 203–23.
113. Michael S. Nolan, *Fundamentals of air traffic control* (Cengage learning, 2011).
114. Mindaugas Lankauskas, „Balansavimas tarp teisės į privatumą ir saviraiškos laisvės Europos žmogaus teisių teismo jurisprudencijoje", *Teisės problemos* 2, 56 (2007): 103–131.
115. Mireille Hildebrandt, „Location Data, Purpose Binding and Contextual Integrity: What's the Message?", 2014, 31–62, https://doi.org/10.1007/978-3-319-05720-0_3; Franck Dumortier, „Facebook and Risks of „De-Contextualization" of Information", *Data Protection in a Profiled World,* sud. Serge Gutwirth, Yves Poullet ir Paul De Hert (Dordrecht: Springer Netherlands, 2010): 119–137, https://doi.org/10.1007/978-90-481-8865-9_7.
116. Monika Zalnieriute, „Big Brother Watch and Others v. the United Kingdom", *American Journal of International Law* 116, 3 (2022): 585–592, https://doi.org/10.1017/ajil.2022.35.
117. Monika Zalnieriute, „Procedural Fetishism and Mass Surveillance under the ECHR", Verfassungsblog: *On Matters Constitutional* (2021).
118. Nadezhda Purtova, „Property rights in personal data", *A European Perspective in Hugenholtz. B.(ed.), Information* (2011).
119. Nick Taylor, „State surveillance and the right to privacy", *Surveillance & Society* 1, 1 (2002): 66–85.
120. Oksana Zabuzhko, „Publicity and Media under Communism and After: The Destruction of Privacy", *Social Research* 69, 1 (2002): 35–47.
121. Oliver Diggelmann ir Maria Nicole Cleis, „How the Right to Privacy Became a Human Right", *Human Rights Law Review* 14, 3 (2014 m. rugsėjo 1 d.): 441–458, https://doi.org/10.1093/hrlr/ngu014.

122. Oliver Jokisch ir kt., „Audio and Video Processing of UAV-Based Signals in the Harmonic Project“, *Studientexte zur Sprachkommunikation: Elektronische Sprachsignalverarbeitung 2021,* (2021), 77–86; Kheireddine Choutri ir kt., „A Multi-Lingual Speech Recognition-Based Framework to Human-Drone Interaction“, Electronics 11, 12 (2022).
123. Paul M. Schwartz, „The EU-US privacy collision: a turn to institutions and procedures“, *Harv. L. Rev.* 126 (2012).
124. Paul McBride, „Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations“, *J. Air L. & Com.* 74 (2009): 627.
125. Paul Ohm, „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“, *UCLA Law Review* 57, 6 (2009): 1701–1778.
126. Petras Tarasevičius, „Teisėsaugos institucijų užduotis kriminalinėje žvalgyboje“, *Teisės problemos* 91, 1 (2016).
127. Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR“, *2019 IEEE International Congress on Big Data (BigDataCongress)* (2019 IEEE International Congress on Big Data (BigData Congress), Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.
128. Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR“, *2019 IEEE International Congress on Big Data (BigDataCongress)* (2019 IEEE International Congress on Big Data (BigData Congress), Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.
129. Prosper Brugière baron de (1782–1866) Auteur du texte Barante, *La Vie Politique de M. Royer-Collard: Ses Discours et Ses Écrits / Par M. de Barante,* 1861, https://gallica.bnf.fr/ark:/12148/bpt6k116929z.
130. Rachel L. Finn ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications“, *Computer Law & Security Review* 28, 2 (2012): 184–194.
131. Rachel L. Finn, David Wright ir Michael Friedewald, „Seven types of privacy“, *European data protection: coming of age* (Springer, 2013), 3–32.
132. Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).
133. Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).
134. Raimundas Kalesnykas ir Vidmantas Mečkauskas, „Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą: teisiniai ir organizaciniai aspektai“, *Jurisprudencija* 36, 28 (2002): 59–70.
135. Ryan Calo, „Against Notice Skepticism in Privacy (and Elsewhere)“, *Notre Dame Law Review* 87 (2011).
136. Ryan Hagemann, „Consumer Privacy in an Age of Commercial Unmanned Aircraft Systems“, *Independent Review* 23, 1 (2018): 9–22;
137. Ryan M. Calo, „The Drone as a Privacy Catalyst“, *Stanford Law Review Online* 64 (2011): 29–33.
138. Richard A. Posner, „The economics of privacy“, *The American economic review* 71, 2 (1981): 405–409.
139. Richard H. Thaler ir Cass R. Sunstein, „Libertarian paternalism“, *American economic review* 93, 2 (2003): 175–179.
140. Richard H. Thaler ir Cass R. Sunstein, *Nudge* (Yale University Press, 2021).
141. Richard Sobel, „The degradation of political identity under a national identification system“, *BUJ Sci. & Tech. L.* 8 (2002): 52.
142. Rob Kitchin, „Big Data, New Epistemologies and Paradigm Shifts“, *Big Data & Society* 1, Nr. 1 (2014 m. liepos 10 d.), p. 5, https://doi.org/10.1177/2053951714528481.
143. Robert Cooter, „Expressive law and economics“, *The Journal of Legal Studies* 27, S2 (1998): 585–607.
144. Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy“, *Technology in Society* 46, Supplement C (2016): 109–119, https://doi.org/10.1016/j.techsoc.2016.03.003.

145. Roger Brownsword ir Morag Goodwin, *Law and the Technologies of the Twenty-first Century: Text and Materials* (Cambridge University Press, 2012); Julia Black, „Critical reflections on regulation“, Austl. J. Leg. Phil. 27 (2002).
146. Roger Brownsword, *Rights, Regulation and the Technological Revolution* (New York: Oxford University Press, Inc., 2008).
147. Roger Clarke, „Understanding the drone epidemic“, *Computer Law & Security Review* 30, 3 (2014): 230–246, https://doi.org/10.1016/j.clsr.2014.03.002; Roger Clarke, „The regulation of civilian drones' impacts on behavioural privacy“, *Computer Law & Security Review* 30, 3 (2014): 286–305, https://doi.org/10.1016/j.clsr.2014.03.005.
148. Roger Clarke, „What drones inherit from their ancestors“, *Computer Law & Seurity Review* 30, 3 (2014): 247–262, https://doi.org/10.1016/j.clsr.2014.03.006.
149. Roland Bénabou ir Jean Tirole, „Incentives and prosocial behavior“, *American economic review* 96, 5 (2006): 1652–1678.
150. Rudolf von Jhering, *Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung,* t. 2 (Breitkopf und Härtel, 1869).
151. Sharifah Mastura Syed Mohd Daud ir kt., „Applications of Drone in Disaster Management: A Scoping Review“, *Science & Justice* 62, 1 (2022): 30–42, https://doi.org/10.1016/j.scijus.2021.11.002.
152. Shaun B. Spencer, „The Surveillance Society and the Third-Party Privacy Problem“, *South Carolina Law Review* 65, 2 (2013).
153. Spyros Kokolakis, „Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon“, *Computers & security* 64 (2017): 122–34.
154. Stephen L. Young ir Michael S. Wogalter, „Comprehension and memory of instruction manual warnings: Conspicuous print and pictorial icons“, *Human Factors* 32, 6 (1990): 637–649.
155. Tamraparni Dasu, Yaron Kanza ir Divesh Srivastava, „Geofences in the sky: herding drones with blockchains and 5G“, *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2018, 73–76.
156. Theodore Reed, Joseph Geis ir Sven Dietrich, „SkyNET: A 3G-Enabled Mobile Attack Drone and Stealth Botmaster“, *WOOT,* 2011, 28–36.
157. Tobias Matzner ir kt., „Do-It-yourself data protection—Empowerment or burden?“, *Data protection on the move* (Springer, 2016): 277–305.
158. Toma Razmaitė, „*Google Street View atvejis:* teisės į privatumą ir technologijų plėtros santykis“ (Vilnius: Mykolo Romerio universitetas, 2014).
159. Toshio Yamagishi, „The provision of a sanctioning system as a public good.“, *Journal of Personality and social Psychology* 51, 1 (1986).
160. Ulrich Bareth, „Privacy-aware and energy-efficient geofencing through reverse cellular positioning“, *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)* (IEEE, 2012): 153–58.
161. Uri Volovelsky, „Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study“, *Computer Law & Security Review* 30, 3 (2014): 306–20, https://doi.org/10.1016/j.clsr.2014.03.008.
162. Valentinas Mikelėnas ir kt., *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys* (Vilnius: Justitia, 2002).
163. William A. Parent, „Recent work on the concept of privacy“, *American Philosophical Quarterly* 20, 4 (1983): 341–55.

Kiti šaltiniai

1. „Aeronautical Knowledge and Safety Test Updates“, template, žiūrėta 2020 m. spalio 14 d., https://www.faa.gov/uas/recreational_fliers/knowledge_test_updates/.
2. „Amazon Hit with Record EU Data Privacy Fine“, *Reuters,* 2021 m. liepos 30 d., posk. Retail & Consumer, https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/.

3. „Bepiločių orlaivių reglamentai ir scenarijai“, žiūrėta 2022 m. gruodžio 2 d., https://ltsa.lrv.lt/lt/veiklos-sritys/oro-transportas-1/bepilociai-orlaiviai/bepilociu-orlaiviu-reglamentai-ir-scenarijai.
4. „BOT | Meaning in the Cambridge English Dictionary“, žiūrėta 2019 m. gegužės 7 d., https://dictionary.cambridge.org/dictionary/english/bot.
5. „China's CCTV Surveillance Network Took Just 7 Minutes to Capture BBC Reporter“, TechCrunch (blog), žiūrėta 2019 m. balandžio 29 d., http://social.techcrunch.com/2017/12/13/china-cctv-bbc-reporter/.
6. „Cyberattacks Against the US Government Up 1,300% Since 2006“, The Fiscal Times, žiūrėta 2019 m. balandžio 30 d., http://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006.
7. „Cookies: GOOGLE fined 150 million euros | CNIL“, žiūrėta 2022 m. gruodžio 6 d., https://www.cnil.fr/en/cookies-google-fined-150-million-euros.
8. „Drone Mapping Applications across Industries“, *Wingtra,* žiūrėta 2022 m. gruodžio 1 d., https://wingtra.com/drone-mapping-applications/.
9. „eBay asks 145 million users to change passwords after data breach – The Washington Post“, žiūrėta 2020 m. rugpjūčio 27 d., https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/.
10. „History of Aviation – First Flights“. Avjobs, Inc. Žiūrėta 2016 m. vasario 15 d. http://www.avjobs.com/history/index.asp.
11. „Hollywood celebrities besieged by drones – and you could be next“, *Mail Online,* 2014 m. rugsėjo 6 d., https://www.dailymail.co.uk/news/article-2746231/Attack-drones-Hollywood-celebrities-besieged-paparazzi-spies-sky-Worried-You-ll-soon-regular-fixture-YOUR-home.html.
12. „How the US Spy Scandal Unravelled“, *BBC News,* 2014 m. sausio 17 d., posk. US & Canada, https://www.bbc.com/news/world-us-canada-23123964.
13. „Yahoo Says 1 Billion User Accounts Were Hacked – The New York Times“, žiūrėta 2020 m. rugpjūčio 27 d., https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
14. „In China, Facial Recognition Tech Is Watching You“, *Fortune,* žiūrėta 2019 m. balandžio 9 d., http://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/.
15. „Industry Leading Drone Market Analysis 2022-2030 | Droneii“, 2022 m. rugsėjo 20 d., https://droneii.com/drone-market-analysis-2022-2030.
16. „Long range directional microphone X64ACS specifications“, žiūrėta 2022 m. gruodžio 16 d., http://ampflab.com/long-range-directional-microphone-X64ACS.html.
17. „M360“, „Kyberfilosofas Alexander Bard: internetas jau perėmė mūsų gyvenimo kontrolę“, žiūrėta 2018 m. spalio 15 d., https://www.delfi.lt/a/78735003.
18. „New Skylogic Research Market Report Uncovers Fresh Insights on Drone Industry“, UAV Coach, 2018 m. rugsėjo 19 d., https://uavcoach.com/skylogic-2018-drone-industry-benchmark/.
19. „Steffi Graf Wins Case v. Microsoft“, AP NEWS, žiūrėta 2022 m. lapkričio 23 d., https://apnews.com/article/0cf8bc65052006588c21b22b4686119a.
20. „The James Bond of Robots: Vijay Kumar at TED2012 | TED Blog“, žiūrėta 2022 m. gruodžio 2 d., https://blog.ted.com/the-james-bond-of-robots-vijay-kumar-at-ted2012/.
21. „Watergate Scandal | Summary, Timeline, & Deep Throat“, *Encyclopedia Britannica,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.britannica.com/event/Watergate-Scandal.
22. „What Did Cambridge Analytica Do During The 2016 Election?“, *NPR.org,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election.
23. „What Is Geofencing? Pros and Cons of Geofencing 2020“, *TSheets,* žiūrėta 2020 m. lapkričio 17 d., https://www.tsheets.com/resources/geofencing-pros-cons.
24. Ben Popken, „Google Sells the Future, Powered by Your Personal Data“, *NBC News,* 2018 m. gegužės 10 d., https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501.

25. *BigRentz,* „6 Ways Drones in Construction Are Changing the Industry – BigRentz“, https://www.bigrentz.com, 2022 m. vasario 16 d., https://www.bigrentz.com/blog/drones-construction.
26. Chris Matyszczyk, „Man Shoots down Drone Hovering over House“, CNET, žiūrėta 2019 m. gegužės 13 d., https://www.cnet.com/news/man-shoots-down-drone-hovering-over-house/.
27. Dana Livonia Contreras ir kt., Unmanned aerial vehicle privacy controls (*Google Patents,* issued 2018 m. sausio 25 d.).
28. David E. Sanger ir kt., „Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing“, *The New York Times,* 2018 m. gruodžio 11 d., https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.
29. Drone Advisory Committee, *Drone Advisory Committee DAC Member eBook,* 2020, https://www.faa.gov/uas/programs_partnerships/drone_advisory_committee/media/Public_Ebook_v3a.pdf.
30. Gabby Robles, „How Drones Are Used in Photography and Cinematography - 42West“, *42 West, the Adorama Learning Center* (blog), 2021 m. gruodžio 10 d., https://www.adorama.com/alc/drones-in-cinematography-photography/.
31. Gabby Robles, „How Police Departments Are Using Drones - 42West, Adorama“, *42 West, the Adorama Learning Center* (blog), 2022 m. birželio 17 d., https://www.adorama.com/alc/police-drones/.
32. Harnil Oza, „How Amazon Used Big Data to Rule E-Commerce? | HData Systems“, žiūrėta 2022 m. lapkričio 25 d., https://www.hdatasystems.com/blog/amazon-used-big-data-ai-to-rule-e-commerce.
33. Insider Intelligence, „Why Amazon, UPS and Even Domino's Is Investing in Drone Delivery Services“, *Insider Intelligence,* žiūrėta 2022 m. gruodžio 1 d., https://www.insiderintelligence.com/insights/drone-delivery-services/.
34. Ishveena Singh, „This Free App Tracks Nearby Drone Flights Using Remote ID Data“, DroneDJ (blog), 2022 m. spalio 4 d., https://dronedj.com/2022/10/04/remote-id-drone-tracking-app/.
35. Jackie Alkobi, „The Evolution of Drones: From Military to Hobby & Commercial“, *Percepto* (blog), 2019 m. sausio 15 d., https://percepto.co/the-evolution-of-drones-from-military-to-hobby-commercial/.
36. James Watkins, *Shut Up and Dance, Drama, Sci-Fi, Thriller (House of Tomorrow,* 2016).
37. JARUS tinklalapis, žiūrėta 2020 m. birželio 22 d., http://jarus-rpas.org/publications.
38. John Sifton, „A Brief History of Drones“, *The Nation,* 2012 m. vasario 27 d., žiūrėta 2016-02-08. Plačiau žr. http://www.thenation.com/article/brief-history-drones/.
39. Jonathan Rupprecht, „FAA Has Busted Multiple Drone Flyers. Here Are The Expensive Results.“, *Forbes,* žiūrėta 2022 m. gruodžio 19 d., https://www.forbes.com/sites/jonathanrupprecht/2022/01/18/faa-busted-multiple-drone-flyers-here-are-the-expensive-results/.
40. Kashmir Hill, „How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did“, Forbes, žiūrėta 2022 m. lapkričio 25 d., https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.
41. Malek Murison, „DJI's Mavic mini is so small you don't have to register it with the FAA“, DRONELIFE (blog), 2019 m. spalio 30 d., https://dronelife.com/2019/10/30/djis-new-mavic-mini-is-so-small-you-dont-have-to-register-it/.
42. Michael Barbaro ir Tom Zeller Jr, „A Face Is Exposed for AOL Searcher No. 4417749“, *The New York Times,* 2006 m. rugpjūčio 9 d., https://www.nytimes.com/2006/08/09/technology/09aol.html.
43. NYU Web Communications, „Independence Blue Cross, NYU, NYU Langone Medical Center Collaborate to Detect Early Diabetes“, žiūrėta 2019 m. balandžio 4 d., http://www.nyu.edu/content/nyu/en/about/news-publications/news/2013/april/independence-blue-cross-nyu-nyu-langone-medical-center-collaborate-to-detect-early-diabetes.

44. *Nordwest-Zeitung,* „Albtraum In Bremen: Drohne schaut ins“, 2018 m. liepos 30 d., https://www.nwzonline.de/bremen/bremen-albtraum-in-bremen-wenn-eine-drohne-ins_a_50,2,481666789.html. (Pora iš Bremeno policijai pateikė pranešimą apie pro miegamojo langą juos stebintį bepilotį orlaivį.);
45. Randy Rieland, „Teaching Drones to Sniff Out Toxic Air“, *Smithsonian Magazine,* žiūrėta 2020 m. rugpjūčio 27 d., https://www.smithsonianmag.com/innovation/teaching-drones-sniff-out-toxic-air-180970231/.
46. Robin Radar Systems, „Why Traditional Radar Isn't Effective at Tracking Drones“, žiūrėta 2022 m. gruodžio 19 d., https://www.robinradar.com/why-traditional-radar-isnt-effective-at-tracking-drones.
47. Sally French, „These 8 States Are the Perfect Sandbox for Drones“, *The Drone Girl* (blog), 2022 m. rugsėjo 29 d., https://www.thedronegirl.com/2022/09/29/drone-sandbox-mercatus/.
48. Sophia Choi, „Atlanta Woman Says Drone 'peeped' on Her While She Dressed“, WSBTV, 2018 m. gegužės 15 d., https://www.wsbtv.com/news/local/atlanta-woman-says-drone-peeped-on-her-while-she-dressed/747083812.
49. Tyler Francke, „Aurora Resident Reports Disturbing Incident of Drone Apparently Spying Through Her Window“, 2019 m. kovo 27 d., https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/, https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/.
50. Von Sabine Norgall, „Drohne spionierte durchs Fenster“, *Mittelbayerische Zeitung,* žiūrėta 2019 m. gegužės 13 d., https://www.mittelbayerische.de/region/regensburg-land-nachrichten/drohne-spionierte-durchs-fenster-21364-art1741147.html.

MYKOLO ROMERIO UNIVERSITETAS

Deividas Kiršys

KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS

Mokslo daktaro disertacijos santrauka
Socialiniai mokslai, teisė (S 001)

Vilnius, 2025

Mokslo daktaro disertacija rengta 2017–2024 m. Mykolo Romerio universitete pagal Mykolo Romerio universitetui su Vytauto Didžiojo universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 „Dėl doktorantūros teisės suteikimo“ suteiktą doktorantūros teisę.

Mokslinė vadovė:

prof. dr. Simona Drukteinienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Mokslo daktaro disertacija ginama Mykolo Romerio universiteto ir Vytauto Didžiojo universiteto teisės mokslo krypties taryboje:

Pirmininkė:

prof. dr. Salvija Mulevičienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Nariai:

doc. dr. Remigijus Jokubauskas (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001);

prof. dr. Jurgita Malinauskaitė (Londono Brunelio universitetas, Jungtinė Karalystė, socialiniai mokslai, teisė, S 001);

prof. dr. Lina Mikalonienė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001);

doc. dr. Saulė Milčiuvienė (Vytauto Didžiojo universitetas, socialiniai mokslai, teisė, S 001).

Mokslo daktaro disertacija ginama viešame Teisės mokslo krypties tarybos posėdyje 2025 m. balandžio 28 d. 13:00 val. Mykolo Romerio universitete, I-414 auditorijoje.

Adresas: Ateities g. 20, 08303 Vilnius.

DEIVIDAS KIRŠYS

KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS

DISERTACIJOS SANTRAUKA

Tyrimo aktualumas ir problematika. Šiuo metu pasaulis išgyvena virsmo laikotarpį, kai beveik kasdien išrandamos technologinės inovacijos, prie kurių reikia greitai prisitaikyti. Pasak profesoriaus Klauso Schwabo, dabar pokyčiai ekonominiame, socialiniame, kultūriniame šiuolaikinės visuomenės gyvenime yra tokie dideli, jog žmonijos istorijoje dar nebuvo tiek daug žadančio, bet ir tiek pavojų keliančio laikotarpio. Šis periodas yra ketvirtosios pramonės revoliucijos pradžia, kuri keičia ne tik kaip mes gyvename, bet ir kas mes esame[649].

Dažnai teigiama, kad teisė nespėja su technologiniais pokyčiais. Vieni tai vadina *tempo problema* (angl. *the pacing problem*[650]), kiti *teisinio reguliavimo ryšio iššūkiu* (angl. *challenge of regulatory connection*[651]), treti lygina su amžinomis lenktynėmis tarp vėžlio ir kiškio, kur teisė atlieka vėžlio, o technologijos – kiškio vaidmenį[652]. Nors teisė tarsi atsilieka nuo technologinių pokyčių, tačiau nuo jų visiškai neatitrūksta, nes inovacijos negali tobulėti be naujų elgesio standartų, o įstatymų leidėjai negali sukurti naujų elgesio standartų be realaus suvokimo, kaip naujas išradimas pakeis socioekonominius santykius.

Teisės aktų pakeitimai nustato naujas elgesio taisykles ir pakeičia ribas to, kas yra priimtina visuomenėje. Taip teisė veikia technologijų vystymąsi. Iš kitos pusės, technologiniai pokyčiai veikia žmonių socialinius ir politinius santykius, keičia atskirų socialinių grupių galios pusiausvyrą, todėl atsiranda naujo teisinio reguliavimo poreikis. Pvz., gali būti nebeaišku, kaip galiojančias taisykles taikyti produktui, paslaugai ar santykiui arba kaip jose klasifikuoti produktą, paslaugą ar santykį. Gali nutikti ir taip, kad galiojančios taisyklės reguliuoja elgesį, kuris tapo nebesvarbus, arba jos buvo sukurtos konkrečiam tikslui pasiekti, bet šis prarado aktualumą ar tapo per brangus įgyvendinti, palyginti su pigesnėmis alternatyvomis[653].

---

649 Klaus Schwab, *The fourth industrial revolution* (New York: Crown Business, 2017), 1–5.

650 Gary E. Marchant, Braden R. Allenby ir Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Dordrecht Heidelberg London New York: Springer Science & Business Media, 2011).

651 Roger Brownsword, *Rights, Regulation and the Technological Revolution* (New York: Oxford University Press, Inc., 2008).

652 Lyria Bennett Moses, „Agents of Change: How the Law 'Copes' with Technological Change", *Griffith Law Review* 20, 4 (2011): 763–794, https://doi.org/10.1080/10383441.2011.10854720.

653 *Ibid.,* 767.

Nors per kelis pastaruosius dešimtmečius žmonių gyvenimus keitė daugybė technologijų, tik kelios jų paskatino peržiūrėti galiojančius teisės aktus. Mokslininkai aktyviai diskutuoja teisiniais klausimais, kylančiais dėl dirbtinio intelekto, biotechnologijos, kriptovaliutos, bet nekreipia dėmesio, kad būtina sureguliuoti, pvz., bevielių ausinių naudojimą. Daugumai naujų technologijų pakanka ir esamo teisinio reglamentavimo, kurį užtikrina bendri gamintojų ir pardavėjų civilinę atsakomybę bei rinkos žaidėjų konkurenciją nustatantys teisės aktai[654]. Kai kurie akademikai inovacijas, kuriomis tik patobulinami ankstesni produkto ar paslaugos atributai, vadina *inkrementinėmis,* o inovacijas, kurios pakeičia egzistuojančius produktus ar paslaugas, – *radikaliomis*[655]. Inkrementiniai išradimai paprastai nesukuria didelės pridėtinės vertės, o radikalios inovacijos kraštutiniais atvejais gali lemti netgi naujos technologinės paradigmos atsiradimą, kuri gali būti naudinga ne tik išradėjui, bet ir visam pasauliui[656].

Bepiločiai orlaiviai, arba *dronai,* patenka į radikalių inovacijų kategoriją. Skaičiuojama, jog 2022 m. bepiločių orlaivių rinkos vertė pasaulyje siekė beveik 31 mlrd. JAV dolerių, iki 2030 m. ji gali pasiekti beveik 56 mlrd.[657]. Paminėtina, kad bepiločiai orlaiviai kariniams tikslams buvo naudojami netgi Pirmajame pasauliniame kare[658], bet tik neseniai, patobulinus šių prietaisų technologijas, jie pradėti naudoti privačiame sektoriuje siuntiniams pristatyti[659], vaizdams fiksuoti[660], žemėlapiams sudaryti[661], statybvietėms kontroliuoti[662]. Bepiločius orlaivius policija naudoja įrodymams rinkti, įtariamųjų ar nelegalių verslų paieškoms[663], gelbėjimo

654 *Ibid.,* 768.

655 Luke A. Stewart, „The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review", *Information Technology & Innovation Foundation,* (2010): 2.

656 *Ibid.,* 2.

657 „Industry Leading Drone Market Analysis 2022-2030 | Droneii", 2022 m. rugsėjo 20 d., https://droneii.com/drone-market-analysis-2022-2030.

658 John Sifton, „A Brief History of Drones", The Nation, 2012 m. vasario 27 d., žiūrėta 2016-02-08. Plačiau žr. http://www.thenation.com/article/brief-history-drones/.

659 Insider Intelligence, „Why Amazon, UPS and Even Domino's Is Investing in Drone Delivery Services", *Insider Intelligence,* žiūrėta 2022 m. gruodžio 1 d., https://www.insiderintelligence.com/insights/drone-delivery-services/.

660 Gabby Robles, „How Drones Are Used in Photography and Cinematography - 42West", *42 West, the Adorama Learning Center* (blog), 2021 m. gruodžio 10 d., https://www.adorama.com/alc/drones-in-cinematography-photography/.

661 „Drone Mapping Applications across Industries", *Wingtra,* žiūrėta 2022 m. gruodžio 1 d., https://wingtra.com/drone-mapping-applications/.

662 *BigRentz,* „6 Ways Drones in Construction Are Changing the Industry – BigRentz", https://www.bigrentz.com, 2022 m. vasario 16 d., https://www.bigrentz.com/blog/drones-construction.

663 Gabby Robles, „How Police Departments Are Using Drones - 42West, Adorama", *42 West, the Adorama Learning Center* (blog), 2022 m. birželio 17 d., https://www.adorama.com/alc/police-drones/.

tarnybos ieško nelaimingų įvykių aukų[664]. Šie maži skraidantys aparatai yra pigūs ir lengvai valdomi, tad juos dažnai įsigyja paprasti vartotojai dėl pramogos ar norėdami pašnipinėti kaimyną[665]. Bepiločių orlaivių technologijai tobulėjant ir atsirandant vis daugiau būdų, kaip juos panaudoti, į padanges turėtų kilti vis daugiau ir įvairių dydžių profesionalų bei mėgėjų valdomų bepiločių orlaivių. Viena bepiločių orlaivių naudojimo grėsmių – privatumo apsauga, šitai pripažįsta daugelis tyrėjų[666].

Bepiločių orlaivių naudojimo taisykles nustato 2019 m. ES priimti reglamentai[667]. Kiek anksčiau, 2016 m., JAV buvo publikuotos nedidelių bepiločių orlaivių naudojimo ir sertifikavimo taisyklės[668]. 2020 m. skelbti rekomendacinio pobūdžio tarptautinių organizacijų dokumentai[669]. Visos iki šiol priimtos taisyklės reglamentuoja tiktai saugų bepiločių orlaivių naudojimą, o problemų, susijusių su privatumu, neliečia. Vienas iš svarbiausių teisės aktų ES, reglamentuojančių privatumo apsaugą, yra Bendrasis duomenų apsaugos reglamentas (toliau – BDAR)[670], tačiau nėra aišku, kiek jis gali sureguliuoti teisinius santykius tarp bepiločių orlaivių valdytojų ir visuomenės.

Neaiškus galiojančių teisės aktų taikymas bepiločių orlaivių naudojimui, privatumo apsaugą užtikrinančio reglamentavimo trūkumas, neapibrėžtas teorinis pagrindas, kaip ateityje reguliuoti privatumą bepiločių orlaivių kontekste, – tai problemos, kurios neleis užtikrinti privataus gyvenimo apsaugos arba trukdys bepiločių orlaivių technologinei pažangai. Disertacijoje, išnagrinėjus dabartinę komercinių bepiločių orlaivių ir privatumo

664 Sharifah Mastura Syed Mohd Daud ir kt., „Applications of Drone in Disaster Management: A Scoping Review“, *Science & Justice* 62, 1 (2022): 30–42, https://doi.org/10.1016/j.scijus.2021.11.002.

665 Tyler Francke, „Aurora Resident Reports Disturbing Incident of Drone Apparently Spying Through Her Window“, 2019 m. kovo 27 d., https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/, https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/.

666 Žr. *infra notes,* 23–32.

667 2019 m. kovo 12 d. Komisijos deleguotasis reglamentas (ES) 2019/945 dėl bepiločių orlaivių sistemų ir trečiųjų valstybių bepiločių orlaivių sistemų naudotojų, C/2019/1821, OJ L 152, 11.6.2019: 1–40 (Reglamentas (ES) 2019/945); 2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos, C/2019/3824, OJ L 152, 11.6.2019: 45–71 (Reglamentas (ES) 2019/947).

668 Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems“, FAA– 2015–0150, Federal Register, 81, 124 (2016): 42064–42214.

669 ICAO model UAS regulations part 101 and 102, (2020); ICAO model UAS regulations part 149, (2020); ICAO Advisory Circular (AC) 101-1, (2020); ICAO Advisory Circular (AC) 102-1, (2020); ICAO Advisory Circular (AC) 102-23, (2020); JARUS UAS Operational Categorization (2019).

670 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119/1, 4.5.2016.

teisinę bazę, taip pat apibendrinus mokslininkų idėjas, siekiama pateikti tokių sprendimų, kurie ateityje būtų pritaikyti teisiniam reguliavimui bei teismų praktikai ir užtikrintų šių dviejų interesų pusiausvyrą.

Darbo objektas – privatumo apsaugos priemonės, taikomos įgyvendinant komercinių bepiločių orlaivių ir privatumo teisinį reguliavimą.

Darbo tikslas – išnagrinėti dabartinį teisinių santykių, kai naudojami bepiločiai orlaiviai, privatumo apsaugos reguliavimą bei specialųjį bepiločių orlaivių reguliavimą ir pateikti jų tobulinimo pasiūlymus.

Siekiant darbo tikslo keliami tokie mokslinio ***darbo uždaviniai:***

7. Apibrėžti bepiločių orlaivių ištakas ir sąvoką, parodyti teisės į privatumą istorines ištakas kontinentinės ir bendrosios teisės tradicijose.

8. Atskleisti teisei į privatumą kylančias grėsmes dėl bepiločių orlaivių naudojimo.

9. Išanalizuoti, kokias privatumo apsaugos priemones siūlo specialusis bepiločių orlaivių reguliavimas.

10. Išnagrinėti, kokias privatumo apsaugos priemones siūlo su privatumu viešoje erdvėje susijęs reguliavimas ir mokslinis diskursas.

11. Išanalizuoti privatumo apsaugos priemones, taikomas reguliuojant teisinę duomenų apsaugą.

12. Pateikti siūlymų dėl bepiločių orlaivių reguliavimo ateityje.

Mokslinio darbo naujumas ir jo reikšmė. Disertacija nauja ir reikšminga šešiais aspektais: visų pirma, mokslinėje literatūroje teigiama, jog bepiločiai orlaiviai kelia grėsmę privatumui, bet konkretūs privatumo pažeidimai detaliau nėra aptariami. Šioje disertacijoje identifikuojama, kokias grėsmes bepiločiai orlaiviai kelia privatumui, ir panaikinama esama spraga mokslinėje literatūroje. Antras aspektas yra tas, kad iki šiol nebuvo atlikta tyrimų, kuriuose būtų analizuojama, kokias privatumo apsaugos priemones suteikia specialusis bepiločių orlaivių reguliavimas. Taigi disertacijoje atliekama ES, JAV ir tarptautinių organizacijų specialiųjų bepiločių orlaivių teisės aktų analizė, kuri leistų nustatyti, ar esamos privatumo apsaugos priemonės yra pakankamos. Trečias, privatumo apsaugos ribos naudojant bepiločius orlaivius labiausiai neaiškios viešojoje erdvėje. Nors mokslinės literatūros gausu, tačiau išsamių tyrimų, aptariančių bepiločių orlaivių naudojimo viešojoje erdvėje problematiką, nėra buvę. Disertacijoje atlikta privatumo viešojoje erdvėje mokslinių šaltinių, teisės aktų bei teismų praktikos analizė itin reikšminga. Ketvirtas, iki šiol nenagrinėta, kokias privatumo apsaugos priemones naudojant bepiločius orlaivius numato ES duomenų apsaugos reguliavimas. Todėl disertacijoje atliekama BDAR analizė, kuri parodo, ar reikia specialiojo naujųjų technologijų, tarp jų ir bepiločių orlaivių, privatumo reguliavimo. Penktas, mokslinėje literatūroje, kuri iki šiol skelbta Lietuvoje, nebuvo tinkamai parodyta paini teisės

į privatumą raida ir kaip skirtingai ji suprantama bendrosios bei kontinentinės teisės tradicijų. Dėl to Lietuvos tyrėjams gali būti sunku suprasti iš esmės skirtingą privatumo apsaugą JAV, kuri dažniausiai aptariama mokslinėje literatūroje. Tai gali lemti tiek klaidingą privatumo koncepcijos interpretaciją, tiek atotrūkį nuo kontinentinės teisės tradicijos, nes dauguma mokslinių straipsnių privatumo teisės klausimais publikuoti būtent JAV autorių. Disertacijoje aptariant teisės į privatumą raidą Prancūzijoje, Vokietijoje, JAV ir Lietuvoje, nagrinėjami privatumo suvokimo skirtumai bendrosios ir kontinentinės teisės tradicijose, bei taip siekiama prisidėti prie kokybiško mokslinio diskurso privatumo tema. Šeštas, apibrėžiant bepiločių orlaivių keliamą grėsmę privatumui ir analizuojant privatumo ribas viešojoje erdvėje remiamasi žinomų teisės srities mokslininkų teorijomis, tad darbo pabaigoje daromos išvados turi tvirtą mokslinį pagrindą. Todėl disertacijoje atliktas tyrimas yra patikimas pagrindas naujoms Lietuvos teisės aktų iniciatyvoms, teismų sprendimams bei tolesniems moksliniams tyrimams, kurie būtų skirti nagrinėti bepiločių orlaivių naudojimo ir teisės į privatų gyvenimą klausimus.

Darbo struktūra. Disertacijos struktūrą sudaro įvadas, keturi skyriai, išvados ir rekomendacijos.

Pirmame skyriuje per galimus privatumo pažeidimus analizuojama, kokią grėsmę privatumui kelia bepiločių orlaivių naudojimas. Skyrių sudaro šeši poskyriai, iš jų pirmieji keturi skirti aptarti bepiločių orlaivius sąvoką ir ištakas bei privatumo koncepciją ir jos ištakas. Toliau penktajame poskyryje analizuojami atskiri privatumo pažeidimai, kuriuos gali sukelti bepiločių orlaivių naudojimas. Šeštame poskyryje pateikiamos skyriaus išvados ir disertacijos autoriaus įžvalgos apie tai, kuo bepiločiai orlaiviai skiriasi nuo kitų privatumą galinčių pažeisti technologijų.

Antras skyrius skirtas specialiųjų bepiločių orlaivių reguliavimo šaltinių analizei. Šiame skyriuje identifikuojamos specialiuosiuose bepiločių orlaivių reguliavimo šaltiniuose randamos privatumo apsaugos priemonės ir detaliai aptariama, kokią privatumo apsaugą kiekviena iš jų galėtų suteikti. Pirmame poskyryje aptariama, kaip disertacijoje suprantama reguliavimo sąvoka. Antrajame aptariami specialieji bepiločių orlaivių reguliavimo dokumentai, juose pateiktos bepiločių orlaivių klasifikacijos. Trečiajame atskirai analizuojamos privatumo apsaugos priemonės, skirtos bepiločiams orlaiviams reguliuoti. Paskutiniame poskyryje daromos skyriaus išvados ir pateikiamos rekomendacijos.

Trečio skyriaus tikslas – išanalizuoti, kokias privatumo apsaugos priemones siūlo su privatumo viešojoje erdvėje problematika susijusi mokslinė literatūra, teisinis reguliavimas ir teismų praktika. Šiame skyriuje nagrinėjamos bendrosios privatumo apsaugos teorijos ir jų taikymo galimybės bepiločių orlaivių kontekste. Skyriuje trys poskyriai: pirmajame aptariama privatumo viešojoje erdvėje problematika; antrajame analizuojama

mokslinė literatūra, skirta privatumui viešojoje erdvėje, ir ieškoma teorinio pagrindo, kaip privatumą viešojoje erdvėje reglamentuoti ateityje; trečiajame – EŽTT ir Lietuvos teismų praktika, susijusi su privatumu viešojoje erdvėje, ir jurisprudencijos vertinimas bepiločių orlaivių kontekste.

Ketvirtame skyriuje analizuojama, kaip bepiločių orlaivių naudojimą reglamentuoja dabartinis ES duomenų apsaugos reguliavimas. Tuo tikslu pirmame poskyryje nagrinėjama, ar BDAR taikomas ir tuomet, kai naudojami bepiločiai orlaiviai. Antrame poskyryje analizuojama, kokiu pagrindu būtų galima teisėtai rinkti duomenis bepiločiu orlaiviu. Trečiame poskyryje aptariama, ar siūlomos BDAR privatumo apsaugos priemonės pakankamos, kad būtų išvengta privatumo pažeidimų dėl bepiločių orlaivių naudojimo. Ketvirtame poskyryje pateikiamas BDAR vertinimas bepiločių orlaivių kontekste. Penktame poskyryje aptariami trūkumai, atsirandantys dėl dabartinės sutikimu paremtos privatumo apsaugos sistemos. Šeštame poskyryje siūloma, kaip ateityje būtų galima keisti privatumo reguliavimą.

Toks struktūrinis sprendimas pasirinktas sąmoningai: pirma nagrinėjamos specialiosios privatumo apsaugos priemonės, kadangi jos yra tiesiogiai taikomos bepiločių orlaivių naudojimui ir yra pagrindinė prevencinė priemonė. Tik po to analizuojami bendrieji privatumo reguliavimo modeliai, kad būtų galima įvertinti, ar egzistuojantis teisinis reguliavimas yra pakankamas ir kokiais aspektais jį galima patobulinti remiantis teoriniais principais. Tokia struktūra leidžia aiškiau nustatyti reguliavimo trūkumus ir siūlyti pagrįstus sprendimus, kurie būtų praktiškai įgyvendinami esamoje teisinėje sistemoje.

Disertacijos pabaigoje pateikiamos išvados, rekomendacijos ir literatūros sąrašas.

Ankstesnių mokslinių tyrimų apžvalga. Disertacijos rengimo laikotarpiu mokslinių tyrimų, visapusiškai atskleidžiančių jos temą, nebuvo. Tačiau daug autorių užsienyje yra paskelbę publikacijų apie bepiločių orlaivių keliamas grėsmes privatumui, iš kurių paminėtini Paulas McBride'as (2009)[671], Ryanas Calo (2011)[672], Rachel Finn ir Dawidas Wrightas (2012)[673], Uri'is Volovelsky'is (2014)[674], Rogeris Clarke'as (2014)[675],

671 Paul McBride, „Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations", *J. Air L. & Com.* 74 (2009): 627.

672 Ryan M. Calo, „The Drone as a Privacy Catalyst", *Stanford Law Review Online* 64 (2011): 29–33.

673 Rachel L. Finn ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 28, 2 (2012): 184–194.

674 Uri Volovelsky, „Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review 30,* 3 (2014): 306–20, https://doi.org/10.1016/j.clsr.2014.03.008.

675 Roger Clarke, „Understanding the drone epidemic", *Computer Law & Security Review* 30, 3 (2014): 230–246, https://doi.org/10.1016/j.clsr.2014.03.002; Roger Clarke, „The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 30, 3 (2014): 286–305, https://doi.org/10.1016/j.clsr.2014.03.005.

Desas Butleris (2014)[676], Margherita Bonetto (2015)[677], Jonathanas P. Westas ir Jamesas S. Bowmanas (2016)[678], Rocci'is Luppicini'is ir Arthuras So (2016)[679]. Vis dėlto pažymėtina, kad išsami analizė, kokiais būdais bepiločiais orlaiviais gali būti pažeidžiamas privatumas, iki šiol nė viename moksliniame darbe nėra atlikta. Apie privatumo apsaugos priemones, taikomas naujuosiuose bepiločių orlaivių ES reglamentuose Nr. 2019/945 ir 2019/947, trumpą straipsnį publikavo Aurelija Pūraitė ir Neringa Šilinskė (2020)[680], kitų mokslinių tyrimų šia tema disertacijos rengimo laikotarpiu nei Lietuvoje, nei užsienyje nebuvo paskelbta. Lietuvoje apie bepiločius orlaivių keliamas grėsmes yra rašęs disertacijos autorius D. Kiršys (2016)[681], taip pat A. Pūraitė, D. Bereikienė ir N. Šilinskė (2017)[682].

Publikacijų, skelbiamų užsienyje teisės į privatumą tema, yra gausu. Teoriniu požiūriu itin aktualūs Danielio Solove'o (2002–2008)[683] tyrimai, skirti teisei į privatų gyvenimą. Taip pat paminėtini R. Finn ir kt. (2013)[684] tyrėjų darbai. Vienu iš disertacijoje analizuojamų pjūvių – pagal istorinę privatumo raidą skirtingose Atlanto pusėse, teisė į privatumą Lietuvoje dar nebuvo analizuota, tuo tarpu užsienyje šį klausimą nagrinėja nemažai autorių, tarp jų aktualiausi Jameso Q. Whitmano (2003)[685], Anupamo Chanderio, Margot'os E. Kaminski ir Williamo McGeverano

676 Des Butler, „The Dawn of the Age of the Drones: An Australian Privacy Law Perspective", *University of New South Wales Law Journal* 37, 2 (2014): 434–470.

677 Margherita Bonetto ir kt., „Privacy in mini-drone based video surveillance", *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG),* 4 (IEEE, 2015), 1–6.

678 Jonathan P. West ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues", *Public Administration Review* 76, 4 (2016): 649–659.

679 Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy", *Technology in Society* 46, Supplement C (2016): 109–119, https://doi.org/10.1016/j.techsoc.2016.03.003.

680 Aurelija Pūraitė ir Neringa Šilinskė, „Privacy Protection in the New Eu Regulations on the Use of Unmanned Aerial Systems", *Public Security and Public Order,* 24 (2020).

681 Deividas Kiršys, „Ar bepiločio orlaivio skrydžio vykdymas žemės sklypo oro erdvėje nepažeidžia to žemės sklypo savininko nuosavybės teisės?" (Vytautas Magnus University, 2016).

682 Aurelija Pūraitė, Daiva Bereikienė ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania", *Baltic Journal of Law & Politics* 10, 2 (2017): 107–132.

683 Daniel J. Solove, „Conceptualizing Privacy", *California Law Review* 90, 4 (2002): 1087–1156; Daniel J. Solove, „Understanding privacy", 2008; Daniel J. Solove, „I've got nothing to hide and other misunderstandings of privacy", *San Diego L. Rev.* 44 (2007): 745; Daniel J. Solove, „A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154, 3 (2006): 477–564; Daniel J. Solove, „Introduction: Privacy self-management and the consent dilemma", *Harv. L. Rev.* 126 (2012): 1880.

684 Rachel L. Finn, David Wright ir Michael Friedewald, „Seven types of privacy", *European data protection: coming of age* (Springer, 2013), 3–32.

685 James Q. Whitman, „The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal* 113, 6 (2004): 1151–1222.

(2020)[686], Paulo Schwartzo (2012)[687], Oliverio Diggelmanno ir Marios Nicole'ės Cleis (2014)[688], Raymondo Wackso (1980)[689], Richardo A. Posnerio (1981)[690], André Bertrand'o (1999)[691], Rudolfo von Jheringo (1869)[692] darbai. Apie teisę į privatų gyvenimą kituose kontekstuose, kurie galėtų būti iš dalies susiję su bepiločių orlaivių naudojimu, Lietuvoje rašė Gediminas Bučiūnas (2010, 2015)[693], Kamilė Mekšriūnaitė (2019)[694], Toma Razmaitė (2014)[695]. Mokslinių publikacijų privatumo viešojoje erdvėje aspektu, Lietuvoje nėra. Todėl atliekant šią tyrimo dalį daugiausia dėmesio skirta užsienio mokslininkų darbams, nors ir juose konkrečiai nerašoma apie bepiločių orlaivių naudojimą, – tai Helen'os Nissenbaum (1998)[696], Joelio R. Reidenbergo (2014)[697], M. E. Kaminski (2015)[698].

BDAR bepiločių orlaivių kontekste nei Lietuvos, nei užsienio tyrėjų išsamiai iki šiol neanalizuotas. Kitais aspektais, kurie gali būti susiję su bepiločių orlaivių naudojimu, BDAR buvo nagrinėtas, pvz., Aurimo Šidlausko (2019)[699], Mamoonos Asghar ir kt. (2019)[700], Jane'ės Andrew ir Maxo Bakerio (2021)[701], Yolos Georgiadou, Rolfo A. de By'aus ir

---

686 Anupam Chander, Margot E. Kaminski ir William McGeveran, „Catalyzing Privacy Law", *Minnesota Law Review* 105, 4 (2021): 1733–1802.

687 Paul M. Schwartz, „The EU-US privacy collision: a turn to institutions and procedures", *Harv. L. Rev.* 126 (2012): 1966.

688 Oliver Diggelmann ir Maria Nicole Cleis, „How the Right to Privacy Became a Human Right", *Human Rights Law Review* 14, 3 (2014 m. rugsėjo 1 d.): 441–458, https://doi.org/10.1093/hrlr/ngu014.

689 Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).

690 Richard A. Posner, „The economics of privacy", *The American economic review* 71, 2 (1981): 405–409.

691 André Bertrand, *Droit à la vie privée et droit à l'image* (Lexis Nexis, 1999).

692 Rudolf von Jhering, *Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung,* t. 2 (Breitkopf und Härtel, 1869).

693 Gediminas Bučiūnas, „Vaizdo registratoriai ir asmens privatumas", *Mokslo taikomieji tyrimai Lietuvos kolegijose* 1, 11 (2015): 64–68; Gediminas Bučiūnas, „Sekimas ir asmens privatumas: kur riba?" (Vilnius: Mykolo Romerio universitetas, 2010).

694 Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu" (Vilnius: Mykolo Romerio universitetas, 2019).

695 Toma Razmaitė, „*Google Street View* atvejis: teisės į privatumą ir technologijų plėtros santykis" (Vilnius: Mykolo Romerio universitetas, 2014).

696 Helen Nissenbaum, „Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy* 17, 5/6 (199): 559–596.

697 Joel R. Reidenberg, „Privacy in Public", *University of Miami Law Review* 69, 1 (2014): 141–160.

698 Margot E. Kaminski, „Regulating Real-World Surveillance", *Washington Law Review* 90, 3 (2015): 1113–1166.

699 Aurimas Šidlauskas, „Video Surveillance and the GDPR", 2019.

700 Mamoona Asghar ir kt., „Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective", *IEEE Access* 7 (2019 m. rugpjūčio 9 d.): 111709–111726, https://doi.org/10.1109/ACCESS.2019.2934226.

701 Jane Andrew ir Max Baker, „The general data protection regulation in the age of surveillance capitalism", *Journal of Business Ethics* 168, 3 (2021): 565–578.

Ouranios Kounadi (2019)[702], Geraldo Spindlerio ir Philippo Schmechelio (2016)[703], Piero A. Bonatti'io ir Sabrinos Kirrane (2019)[704] darbuose.

Apibendrinant galima teigti, kad nei Lietuvoje, nei užsienyje iki šiol nėra tyrimų, kurie atskleistų bepiločių orlaivių naudojimo keliamą grėsmę privatumui. Taip pat nėra mokslinių straipsnių, kurie identifikuotų ir išsamiai analizuotų, kaip specialiuosiuose bepiločių orlaivių reguliavimo šaltiniuose apibrėžtos privatumo apsaugos priemonės. Nėra ir mokslinių publikacijų, kuriose būtų analizuojama, kaip BDAR taikomas bepiločiams orlaiviams.

Mokslinio tyrimo metodologija. Rengiant šią disertaciją buvo taikyti keli mokslinio tyrimo metodai.

Dokumentų analizės metodas naudotas pirminiams informacijos šaltiniams atrinkti ir suprasti. Analizuoti duomenų šaltiniai gali būti grupuojami į keturias pagrindines kategorijas. Pirma, Lietuvos ir užsienio tyrėjų moksliniai darbai, aprašantys bepiločių orlaivių naudojimą. Antra, teoriniai moksliniai darbai, susiję su teise į privatų gyvenimą. Trečia, moksliniai darbai, teismų praktika ir teisės aktai, skirti privatumui viešojoje erdvėje. Ketvirta, moksliniai darbai, teisės aktai ir teismų praktika, susijusi su ES duomenų apsaugos reglamentavimu.

Renkant duomenis tyrimui naudotasi Mykolo Romerio universiteto bibliotekos ištekliais bei prenumeruojamomis duomenų bazėmis, taip pat užsienio valstybių bibliotekų fondais ir universitetų duomenų bazėmis, moksliškai patikimais elektroniniais leidiniais. EŽTT, LAT praktikos ieškota per platformas „Infolex", „eTeismai", „Liteko", duomenų bazėje „HUDOC". Lietuvos ir užsienio valstybių teisės aktų ieškota oficialiuose jų įstatymų leidžiamosios valdžios, teisės aktų skelbimo tinklalapiuose.

Istorinis metodas taikytas istorinėms prielaidoms, leidusioms susiformuoti tokiems moderniems bepiločiams orlaiviams, kokie šiais laikais naudojami, atskleisti. Šis metodas taip pat naudotas siekiant parodyti teisės į privatų gyvenimą ištakas Prancūzijoje, Vokietijoje, JAV ir Lietuvoje.

Sisteminės analizės metodas. Taikant šį metodą bendrasis privatumo ir specialusis bepiločių orlaivių reglamentavimas išnagrinėtas sistemiškai, atskleidžiant jų naudojimo ir privatumo santykį.

---

702 Yola Georgiadou, Rolf A. de By ir Ourania Kounadi, „Location Privacy in the Wake of the GDPR", *ISPRS International Journal of Geo-Information* 8, 3 (2019): 157, https://doi.org/10.3390/ijgi8030157.

703 Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): [i]-177.

704 Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR", *2019 IEEE International Congress on Big Data (BigDataCongress)* (2019 IEEE International Congress on Big Data *(BigData Congress),* Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.

Palyginamoji analizė atlikta siekiant nustatyti skirtingose teisės sistemose susiformavusį privatumo suvokimą, specialiųjų bepiločius orlaivius reglamentuojančių teisės aktų nuostatas skirtingų organizacijų priimtuose dokumentuose, privatumo viešojoje erdvėje teorijas.

Analitinis kritinis metodas taikytas reaguojant į skirtingų organizacijų priimto specialiojo bepiločių orlaivių reguliavimo, EŽTT ir Lietuvos teismų praktikos, ES duomenų apsaugos teisės aktų trūkumus bei jų įgyvendinimo sunkumus, taip pat mokslinėje literatūroje siūlomų teisinio reguliavimo sprendimų trūkumus.

Ginamieji teiginiai

1. Bepiločiai orlaiviai pasižymi savybėmis, kurių neturi jokia kita iki šiol naudota privatumą galinti pažeisti technologija – ji prisideda prie ribų tarp virtualaus ir realaus pasaulio nykimo, gali būti plačiai naudojama, leidžia vykdyti intensyvią stebėseną įvairiais kampais, turi potencialą būti panaudota kaip ginklas ir yra sunkiai pastebima. Todėl ES, JAV ir tarptautinis specialusis bepiločių orlaivių reguliavimas, orientuotas labiau į saugumo užtikrinimą ir paremtas savarankiško privatumo valdymo paradigma, yra nepakankamas siekiant tinkamai apsaugoti privatumą ir sukuria poreikį specialiojo reguliavimo tobulinimui.

2. Dabartinė teisinė privatumo apsaugos sistema yra paremta savarankiško privatumo valdymo paradigma. Siekiant efektyvesnės privatumo apsaugos bepiločių orlaivių naudojimo kontekste, kuriant jų reguliavimą ateityje reikėtų vadovautis paternalistine ribų valdymo teorija.

Išvados. Apibendrindamas atliktą mokslinį tyrimą disertacijos autorius konstatuoja, kad įvade nurodytas disertacinio tyrimo tikslas pasiektas, išsikelti uždaviniai įgyvendinti, o ginamieji teiginiai patvirtinti. Tai pagrindžia toliau pateikiamos tyrimo išvados:

1. Disertacijoje atliktas tyrimas atskleidė, jog bepiločiai orlaiviai grėsmę privatumui kelia per tokius pažeidimus kaip stebėsena, agregavimas, identifikavimas, saugumo neužtikrinimas ir atidengimas. Šių pažeidimų grėsmė kyla, nes bepiločių orlaivių technologija turi išskirtinių savybių, kurių neturi nė viena iki šiol prieinama stebėsenos priemonė. Tai tokios savybės kaip didelis panaudojimo mastas, stebėjimo intensyvumas, stebėjimo kampų įvairovė, galimybė tapti ginklu ir nepastebimumas. Kaip parodė atliktas tyrimas, išskirtinės bepiločių orlaivių galimybės įgalina tiek valstybes, tiek didelę galią rinkoje turinčius subjektus kurti infrastruktūrą oportunistiniam informacijos rinkimui realiame pasaulyje, todėl tinkamai nereglamentuojant bepiločių orlaivių naudojimo galimas atšalimo efektas, t. y. nepageidaujami žmonių psichikos pokyčiai, socialinių grupių ir skirtingų visuomenės sluoksnių elgsenos pakitimai į blogąją pusę, grėsmė demokratinės santvarkos stabilumui.

2. Iš nagrinėtų specialiųjų bepiločių orlaivių reguliavimo šaltinių, kuriuos yra priėmę ICAO, JARUS, ES ir JAV, matyti, jog *expressis verbis* privatumo apsaugą įtvirtina tik ES bepiločių orlaivių reglamentai. Vis dėlto tai nereiškia, jog kiti nagrinėti šaltiniai privatumo apsaugos priemonių nenumato – juose apsaugos priemonės įtvirtintos netiesiogiai. Atlikta analizė parodė, jog dabartiniuose specialiuosiuose bepiločių orlaivių teisės aktuose egzistuoja šios prevencinės priemonės, kurios galėtų padėti išvengti privatumo pažeidimų: (a) reikalavimas laikytis atstumo; b) reikalavimas informuoti / gauti sutikimą; (c) registracijos reikalavimas; (d) reikalavimas kaupti įrašus; (e) kvalifikacijos reikalavimus bepiločių orlaivių pilotams; (f) reikalavimai atlikti rizikos vertinimą; (g) nuotolinio identifikavimo priedai; (h) geografinio orientavimo priedai (geografinis apribojimas); (i) duomenų perdavimo ryšio linijos saugumo užtikrinimas; (j) reikalavimas bepiločius orlaivius gaminti su žibintais. Disertacijos autoriaus vertinimu, visos aptartos priemonės vienokiu ar kitokiu būdu teoriškai galėtų sumažinti privatumo pažeidimų tikimybę, tačiau daugelis jų šiuo metu realios prevencijos neužtikrina dėl reglamentuojančiuose nuostatuose esančių trūkumų ir nepakankamo privatumą saugančių technologijų išsivystymo.

3. Atlikus privatumo viešojoje erdvėje mokslinės literatūros analizę buvo identifikuotos trys moksliniame diskurse vyraujančios teorijos, kurių pagrindu užsienio autoriai siūlo reguliuoti privatumo ribas viešojoje erdvėje: (i) *kontekstinio integralumo teorija,* (ii) *visuomeninės reikšmės teorija* ir (iii) *ribų valdymo teorija.* Kiekviena jų buvo analizuojama, siekiant nustatyti, ar kuri nors iš jų sukurtų pusiausvyrą tarp privatumo viešojoje erdvėje ir technologinės pažangos. Atliktas tyrimas parodė, jog *kontekstinio integralumo teorija* nesuteiktų pakankamos privatumo apsaugos nuo pažeidimų, kuriuos gali sukelti nedidelių bepiločių orlaivių naudojimas. Ją taikant nagrinėjamas jau surinktos informacijos tolesnio perleidimo ir lyginimo teisėtumas, tačiau pats duomenų rinkimo faktas nėra svarbus, o bepiločių orlaivių kontekste kaip tik sureguliuoti duomenų rinkimo teisėtumą būtų svarbiausia. Disertacijos autoriaus vertinimu, *visuomeninės reikšmės teorija* taip pat nesuteiktų tinkamos apsaugos privatumui. Ją taikant aiškintis, kuri teisė viršesnė – teisė į privatumą ar teisė į saviraišką, teismai būtų per daug apkraunami. Šis reguliavimo modelis beveik nesuteikia jokios pridėtinės vertės, palyginti su pasenusia dvinare teorija, kuriai svarbiausia, ar informacija buvo surinkta viešojoje ar privačioje erdvėje, t. y. teritorinė viešosios ir privačios erdvės perskyra. Galiausiai *ribų valdymo teorijos* taikymas, disertacijos autoriaus nuomone, turėtų supaprastinti įstatymų leidybos procesą, palengvinti teisminius ginčus, kylančius dėl bepiločių orlaivių naudojimo, pernelyg nesuvaržyti bepiločių orlaivių technologinio vystymosi. Šio modelio taikymas taip pat turėtų skatinti visuomenės įsitraukimą į sprendimų priėmimą teisinio reguliavimo procese, skatinti visuomenės individualų bei grupinį savarankiškumą, autonomiškumą, todėl atitinkamai turėtų padėti išvengti atšalimo efekto.

4. EŽTT ir LAT praktikos, susijusios su privatumo ribomis viešojoje erdvėje, analizė atskleidė, jog bylų, nagrinėjančių bepiločių orlaivių naudojimą, teismai iki šiol nėra sprendę. Kasacinio teismo jurisprudencijoje su privatumu susijusių bylų apskritai nėra daug, jose negausu universalaus taikymo teisės taisyklių, todėl iš esamos praktikos daryti išvadas apie tolesnę Lietuvos teismų sprendimų motyvaciją, iškilus byloms bepiločių kontekste, būtų pernelyg drąsu. Iš EŽTT jurisprudencijos, kuria privalo vadovautis ir Lietuvos teismai, matyti reikšmingai skirtingas privatumo viešojoje erdvėje ribų vertinimas, priklausomai nuo to, koks subjektas vykdo stebėseną – privatus asmuo ar valdžios institucija. Pagal suformuotą praktiką privačių subjektų bepiločiais orlaiviais vykdoma stebėsena turėtų būti kur kas labiau prižiūrima ir reguliuojama, tačiau esama praktika pernelyg abstrakti, kad ja teisėjai bepiločių orlaivių naudojimo ir privatumo santykio bylose galėtų vadovautis be papildomo teorinio pagrindo. Tokį teorinį pagrindą suteikia siūloma ribų valdymo teorija, kuri būtų suderinama su EŽTT jau suformuotomis universalaus taikymo taisyklėmis. Valdžios institucijų viešojoje erdvėje vykdoma stebėsena bepiločiais orlaiviais pagal suformuotą EŽTT praktiką beveik nebūtų ribojama dėl neseniai priimto masinės stebėsenos režimui palankaus sprendimo byloje „Big Brother Watch and Others v. the United Kingdom“, kuriuo remiantis valstybėms suteikiama plati diskrecija pasirinkti, kiek bus varžomas asmenų privatumas siekiant nacionalinio saugumo. Disertacijos autoriaus manymu, slapta masinė stebėsena, nesvarbu, kas ją vykdo, valdžios institucijos ar privatūs asmenys, iš materialiosios teisės perspektyvos, visais atvejais būtų nesuderinama su ribų valdymo teorija ir lemtų privatumo pažeidimus, nes stebimi asmenys, nežinodami apie jų atžvilgiu vykdomą stebėseną, negali keisti savo elgesio. Manytina, jog šiuo metu vienintelis dalykas, galintis sustabdyti slaptos bepiločiais orlaiviais vykdomos stebėsenos taikymą, yra stipri tarptautinė arba nacionalinė politinė valia atsisakyti masinės valstybės institucijų vykdomos stebėsenos. Kaip parodė atliktas tyrimas, šiuo požiūriu Lietuvos teisės aktai, nors ir kritikuojami Lietuvos teismų, keičiami privatumui nepalankia linkme.

5. Kaip parodė atlikta ES duomenų teisės aktų analizė, į BDAR reguliavimo sritį bepiločiai orlaiviai patenka, nes tai įrankis duomenims rinkti. BDAR bepiločių orlaivių vykdomam duomenų rinkimui nebūtų taikomas tik tais atvejais, kai iš surinktos medžiagos asmenų neįmanoma identifikuoti, arba tada, kai duomenys pateikiami anonimiškai. Iš teisėtų duomenų tvarkymo pagrindų, kuriais galėtų vadovautis bepiločių orlaivių valdytojai, disertacijos autoriaus nuomone, labiausiai tikėtini yra duomenų subjekto sutikimas (BDAR 6 straipsnio 1 dalies a punktas) ir „teisėtas interesas“ (BDAR 6 straipsnio 1 dalies f punktas). Disertacijos autorius identifikavo dar vieną realų duomenų bepiločiais orlaiviais rinkimo pagrindą, kurio *expressis verbis* BDAR nenumato, tai – nacionalinis teisės aktas. Atlikta analizė parodė, jog pagal ESTT praktiką, suformuotą stacionarių CCTV

kamerų kontekste, net ir paprasti vartotojai, vykdydami skrydį viešoje vietoje, turėtų gauti aplinkinių sutikimą. Vis dėlto, disertacijos autoriaus vertinimu, BDAR nuostatų tikriausiai nereikėtų taikyti vidutiniams vartotojams, vykdantiems skrydžius asmeniniais tikslais, todėl šia ESTT praktika vadovautis nebūtų tikslinga.. Vertinant BDAR siūlomas privatumo apsaugos priemones prieita prie išvados, jog didžiausią naudą suteikia šifravimo sprendimai ir poveikio duomenų apsaugai vertinimai. Kaip vienas iš šifravimo sprendimų, atskirai aptartas anonimiškumas, kuriuo apdoroti duomenys į BDAR taikymo sritį nepatektų. Tiesa, šiuo metu anonimizavimo technologija nėra pakankamai išsivysčiusi, todėl negalėtų būti plačiai taikoma. Taip pat kritikuotina, jog dabartiniai teisės aktai nenumato anonimizuotų duomenų saugojimo termino, o tai sudaro dingstis piktnaudžiauti. Kitos BDAR numatytos privatumo apsaugos garantijos abstraktesnio pobūdžio, bet taip pat reikšmingai prisideda prie privatumo apsaugos, nes veikia kaip standartizavimo šaltinis, kuriuo vadovaudamiesi bepiločių orlaivių rinkos dalyviai gali užsiimti kryptinga savireguliacija. Taigi sutikimas – pagrindinis ES duomenų apsaugos režimo ramstis, todėl BDAR, neskaitant kai kurių naudingų numatytų konkrečių privatumo apsaugos priemonių, privatumo apsauga, paremta savarankiško *privatumo valdymo paradigma,* būtų neveiksminga privatumo apsaugai bepiločių orlaivių naudojimo kontekste.

6. Savarankiškas privatumo valdymas, paremtas individo sutikimu, turi trūkumų. Duodami sutikimą tvarkyti duomenis, žmonės dažnai nesupranta realių savo pasirinkimo pasekmių arba jas supranta kiek iškreiptai dėl įgimto riboto racionalumo. Taip pat galima teigti, jog individai šių dienų rinkos sąlygomis neturi realios autonomijos priimti sprendimus, nes verslo modelių, pagal kuriuos būtų renkama mažiau duomenų, ekonomikoje tiesiog nėra, Žmonės taip pat neturi laiko skaityti privatumo politikų, tiksliai nenumato ilgalaikių duomenų tvarkymo ir derinimo tarpusavyje (agregavimo) pasekmių. Viena mokslinėje literatūroje siūlomų išeičių – paternalistinis reguliavimas, kuriuo iš esmės suvaržoma individo pasirinkimo laisvė dėl jo paties gerovės. Paternalistinių nuostatų apstu įvairiuose šiuolaikiniuose teisės aktuose, tai būdinga ir BDAR, ir specialiajam bepiločių orlaivių reguliavimui. Disertacijos autoriaus siūlomas bepiločių orlaivių reguliavimo modelis taip pat paternalistinis. Jis paremtas ne sutikimu, o privalomo pobūdžio elgesio taisyklėmis, kurios nustatomos vadovaujantis formaliu reguliavimu. Pagrindinis dalykas, kuris daro šį reguliavimo modelį patrauklų, yra jo paprastumas. Jo taikymas leistų palengvinti teismų darbą, o per diskusijas dėl to, kaip turėtų būti reguliuojamas privatumas viešojoje erdvėje, įtrauktų plačiąją visuomenę. Disertacijos autoriaus vertinimu, siūlomas reguliavimas galėtų būti įgyvendintas per formalų reguliavimą, reguliavimą informuojant ir standartizavimą.

Daugiau disertacijos autoriaus vertinimų dėl problemų, kylančių naudojant bepiločius orlaivius, pateikta pačiame darbe.

Rekomendacijos

1. ES reglamentai Nr. 2019/945 ir 2019/947 numato privalomus nuotolinio identifikavimo priedus daugeliui bepiločių orlaivių. Skrydžio identifikavimo duomenų transliavimas šiuo metu privalomas tik vietiniu būdu (radijo ryšiu), o tai apsunkina pažeidimų nustatymą, kai bepiločiais orlaiviais vykdoma slapta stebėsena. Išeitis galėtų būti identifikavimo duomenų transliavimas ne tik radijo ryšiu, bet ir internetu centrinei valdžios institucijai. Vis dėlto, kaip galima spręsti iš pastarųjų metų JAV patirties, šį pasiūlymą įgyvendinti šiuo metu būtų sudėtinga dėl nepakankamo nuotolinio identifikavimo technologijos išsivystymo. Taigi ES teisės aktų leidėjai į šį pasiūlymą turėtų atsižvelgti ateityje rengdami bepiločių orlaivių reglamentavimą, kai nuotolinio identifikavimo priedų technologija bus labiau išvystyta.

2. ES reglamentai Nr. 2019/945 ir 2019/947 numato reikalavimą saugoti įrašus apie vykdomą skrydį bepiločiu orlaiviu. Ši priemonė padėtų užtikrinti tam tikrą privatumo apsaugą, bet pagal dabartinį ES reguliavimą kaupiamų duomenų apimtis yra nepakankama, kad tai būtų veiksminga. Disertacijos autorius rekomenduoja kaupti daugiau asmens duomenų, kad iš jų būtų galima atkurti įvykdyto pažeidimo detales. Didinant kaupiamų duomenų apimtį, turėtų būti laikomasi šių sąlygų: 1) duomenys būtų tik bepilotyje orlaivyje, jie nebūtų pasiekiami internetu (juodosios dėžės), 2) duomenys tretiesiems asmenims būtų teikiami tik pagal teisėtą įgaliotos valdžios institucijos (teismo, ikiteisminio tyrimo pareigūno ar kt.) pareikalavimą, 3) duomenims būtų nustatytas konkretus ribotas saugojimo terminas.

3. ES reglamentai Nr. 2019/945 ir 2019/947 numato, jog bepiločiai orlaiviai, kurių svoris nesiekia 250 g, neprivalo turėti nuotolinio identifikavimo priedų. Ateityje daugiausia problemų dėl privatumo kels būtent nedideli bepiločiai orlaiviai, kurie be nuotolinio identifikavimo priedų nuotoliniu būdu bus neatpažįstami nukentėjusiems tretiesiems asmenims ar teisėsaugos institucijoms. Atsižvelgiant į tai, rekomenduotina keisti ES specialųjį bepiločių orlaivių reguliavimą, numatant, kad nuotolinius identifikavimo priedus būtų privaloma sieti ne tik su svoriu, bet ir analogiškai, kaip yra ES bepiločių orlaivių registracijos nuostatuose, su galimybe fiksuoti asmens duomenis. Tai, kad nuotoliniai identifikavimo priedai yra privalomi, galėtų būti siejama ir su registracijos reikalavimu (jei bepilotis registruotinas, jis turėtų turėti ir nuotolinio identifikavimo priedą).

4. ES reglamentai Nr. 2019/945 ir 2019/947 numato reikalavimą gaminti bepiločius orlaivius su žibintais. Dabartinis reguliavimas taiko išimtį bepiločiams orlaiviams, kurių svoris nesiekia 250 g, tačiau ir tokio svorio ar lengvesni bepiločiai orlaiviai gali pažeisti privatumą. Ateityje nedideliais bepiločiais orlaiviais privatumą pažeisti bus dar lengviau. Žibintai yra viena lengviausiai įgyvendinamų, pigiausių ir veiksmingiausių priemonių,

galinčių apsaugoti privatumą. Todėl reikalavimas gaminti bepiločius orlaivius su žibintais turėtų būti taikomas visiems, kurie gali fiksuoti asmens duomenis, neatsižvelgiant į tai, ar skrydis vykdomas dienos ar nakties metu. Įgyvendinant šį pasiūlymą reikėtų nustatyti, kad bepiločių orlaivių šviesos šaltinis būtų tokio stiprumo, jog būtų matomas bent iš atstumo, kuris galėtų veiksmingai apsaugoti privatumą ir atkreiptų pašalinių asmenų dėmesį netgi saulėtą dieną.

5. Kai asmens duomenys komerciniu tikslu renkami bepiločiu orlaiviu, pagal ES teisinį reguliavimą jo valdytojai privalo dar prieš skrydį gauti duomenų subjektų sutikimus. Iki atsirandant bepiločiams orlaiviams, sutikimas kaip privatumo apsaugos priemonė buvo dažniausiai naudojamas savarankiškam privatumo valdymui internete, tačiau šią priemonę pritaikyti bepiločiams orlaiviams sunku, nes jo valdytojui gauti sutikimą kiekvieną kartą prieš skrydį būtų sudėtinga. Dėl to, kad nėra pritaikytos teisinės bazės, ilgainiui tai gali tapti kliūtimi technologinei bepiločių orlaivių pažangai. Kaip išeitį disertacijos autorius rekomenduotų, kad teisėkūra ir teismai ateityje vadovautųsi paternalistinio pobūdžio ribų valdymo teorija, kuri paremta ne sutikimu, o privalomo pobūdžio elgesio taisyklėmis, nustatytomis vadovaujantis formaliu reguliavimu.

6. Daugelis šiais laikais prieinamų anonimizavimo technologijų turi imanentinių trūkumų, dėl kurių patikimai anonimizuoti duomenis šiuo metu neįmanoma. Nepaisant to, jog anonimišką informaciją jau įmanoma deanonimizuoti, teisės aktuose nėra numatyti tokių duomenų saugojimo terminai. Šia teisės aktų spraga gali pasinaudoti didžiųjų duomenų valdytojai sukeldami grėsmę privatumui per agregavimo, saugumo neužtikrinimo ir identifikavimo pažeidimus. Disertacijos autorius rekomenduotų teisės aktuose nustatyti anonimizuotų duomenų saugojimo terminą.

MOKSLINIO TYRIMO REZULTATŲ APROBAVIMAS IR SKLAIDA

Dalis disertacijoje atlikto tyrimo buvo paskelbta mokslo žurnaluose „Baltic Journal of Law & Politics“ bei „Teisės apžvalga“, mokslinėje knygoje „Future law, ethics, and smart technologies: the future of legal education“:

Kiršienė, Julija, Christopher Kelley, Deividas Kiršys ir Juras Žymančius. „Rethinking the Implications of Transformative Economic Innovations: Mapping Challenges of Private Law“. Baltic Journal of Law & Politics 12, 2 (2019): 47–77.

https://cris.mruni.eu/cris/handle/007/16404

Kiršys, Deividas, „Dronų grėsmė privatumui: galimi pažeidimai“, Teisės apžvalga, 1 (2021): 64–87.

https://cris.mruni.eu/cris/handle/007/48404

Kiršienė, J., Gruodytė, E., & Kiršys, D. (2023). Transformative Smart Technologies: Mapping Challenges of Private Law. In Future Law, Ethics, and Smart Technologies (pp. 30-47). Brill.

https://cris.mruni.eu/cris/handle/007/48403

Dalis tyrimo rezultatų taip pat pristatyta mokslo renginiuose:

2020 m. vasario 20 d. skaitytas pranešimas tema „Do drones infringe on our right to privacy?“ tarptautinėje mokslinėje konferencijoje „Future Law, Ethics, and Smart Technologies“.

2020 m. lapkričio 6 d. skaitytas pranešimas tema „Ar dronų naudojimas pažeidžia teisę į privatumą“ VDU Teisės fakulteto rengiamose dirbtuvėse „Teisinės problemos skaitmeninėje visuomenėje“.

GYVENIMO APRAŠYMAS

Vardas: Deividas
Pavardė: Kiršys

Išsilavinimas

2017 – 2024	Mykolo Romerio universitetas, Teisės mokykla, doktorantūros studijos
2015 – 2015	Liuksemburgo universitetas, ERASMUS studentas Europos Sąjungos teisės magistro studijų programoje
2011 – 2016	Vytauto Didžiojo universitetas, Teisės magistro laipsnis
2011 – 2016	JAV Mičigano Valstijos universitetas, Transnacionalinės teisės sertifikatas
2011 – 2016	Vytauto Didžiojo universitetas, Politikos mokslų gretutinės studijos

Darbo patirtis

2023 – Dabar	Teisės ir atitikties vadovas, UAB „TV Žaidimai“
2021 – 2022	Teisininkas, Citco Mercator, UAB
2020 – 2021	Advokato padėjėjas, APB „Čerka ir partneriai“
2018 – 2021	Teisininkas / mediatorius, individuali veikla
2018 – 2020	Narys, Lietuvos administracinių ginčų komisijos Šiaulių apygardos skyrius
2016 – 2017	Teisininkas, Šiaulių m. 4-asis notarų biuras
2015 – 2016	Teisininkas, APB „Magnusson ir partneriai“

Kita

2015 – 2016	Revizijos komisijos narys, Europos Studentų Teisininkų asociacijos Lietuvos skyrius
2014 – 2015	Prezidentas, Europos Studentų Teisininkų asociacijos Vytauto Didžiojo universiteto skyrius
2013 – 2014	Viceprezidentas STEP, Europos Studentų Teisininkų asociacijos Vytauto Didžiojo universiteto skyrius

MYKOLAS ROMERIS UNIVERSITY

Deividas Kiršys

USE OF COMMERCIAL DRONES AND PRIVACY PROTECTION: LEGAL CHALLENGES AND REGULATORY IMPROVEMENT GUIDELINES

Summary of Doctoral Dissertation
Social Sciences, Law (S 001)

Vilnius, 2025

The doctoral dissertation was prepared between 2017 and 2024 and is defended at Mykolas Romeris University, in accordance with the authority granted by Order No. V-160 of the Minister of Education, Science and Sport of the Republic of Lithuania, dated 22 February 2019.

Scientific Supervisor:

Prof. Dr. Simona Drukteinienė (Mykolas Romeris University, Social Sciences, Law, S 001).

The defense of the doctoral dissertation will take place before the Defense Board in the Field of the Science of Law of Mykolas Romeris University and Vytautas Magnus University, with the following members:

Chairperson:

Prof. Dr. Salvija Mulevičienė (Mykolas Romeris University, Social Sciences, Law, S 001).

Members:

Assoc. Prof. Dr. Remigijus Jokubauskas (Mykolas Romeris University, Social Sciences, Law, S 001);

Prof. Dr. Jurgita Malinauskaitė (Brunel University of London, United Kingdom, Social Sciences, Law, S 001);

Prof. Dr. Lina Mikalonienė (Mykolas Romeris University, Social Sciences, Law, S 001);

Assoc. Prof. Dr. Saulė Milčiuvienė (Vytautas Magnus University, Social Sciences, Law, S 001).

The doctoral dissertation defense will take place during a public meeting of the Law Science Field Council on April 28, 2025, at 1:00 PM at Mykolas Romeris University, auditorium I-414.

Address: Ateities St. 20, 08303 Vilnius, Lithuania.

DEIVIDAS KIRŠYS

USE OF COMMERCIAL DRONES AND PRIVACY PROTECTION: LEGAL CHALLENGES AND REGULATORY IMPROVEMENT GUIDELINES

SUMMARY

Relevance and Research Problems

The world is currently undergoing a transformative phase characterized by the rapid emergence of technological innovations. This dynamism demands swift adaptability. Professor Klaus Schwab underscores the magnitude of changes in economic, social, and cultural realms, noting both the promise and peril of this era. This epoch signifies the inception of the fourth industrial revolution, reshaping not only our lifestyle but also our identity[711].

A recurrent notion asserts that the law lags behind technological evolution. Dubbed the "pacing problem,"[712] the challenge of regulatory connection[713], or even likened to the fable of the tortoise and the hare[714], law's slow progress contrasts with technology's rapid advancement. However, law is not entirely detached from technology. Innovations necessitate new standards of conduct, while legislators require a profound comprehension of how these innovations reshape socioeconomic dynamics.

Legislative changes establish new behavioral norms and redefine societal boundaries. This reciprocal relationship influences technology's evolution. Conversely, technological shifts alter social and political dynamics, leading to calls for new legal frameworks. Often, existing rules struggle to accommodate new products, services, or relationships. Some may become obsolete, irrelevant, or excessively costly to uphold compared to newer alternatives[715].

While numerous technologies have reshaped lives, only a few prompt the revision of existing laws. Debates among scholars concerning legal implications of artificial intelligence, biotechnology, and cryptocurrency tend to overshadow the need to regulate seemingly mundane aspects, such as wireless headphones. For most new technologies, prevailing regulations suffice, driven by manufacturers' civil liability and competition laws. Some classify innovations as either

711 Klaus Schwab, *The fourth industrial revolution* (New York: Crown Business, 2017), 1–5.
712 Gary E. Marchant, Braden R. Allenby ir Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Dordrecht Heidelberg London New York: Springer Science & Business Media, 2011).
713 Roger Brownsword, *Rights, Regulation and the Technological Revolution* (New York: Oxford University Press, Inc., 2008).
714 Lyria Bennett Moses, „Agents of Change: How the Law 'Copes' with Technological Change", *Griffith Law Review* 20, 4 (2011): 763–794, https://doi.org/10.1080/10383441.2011.10854720.
715 *Ibid.,* 767.
716 *Ibid.,* 768.

incremental, enhancing prior attributes, or radical, replacing existing paradigms[717]. Incremental changes often offer marginal value, while radical innovations may usher in new technological epochs with global benefits[718].

Unmanned aerial vehicles, or drones, exemplify radical innovation. In 2022, the global drone market value reached nearly $31 billion, projected to exceed $56 billion by 2030[719]. While drones trace their roots back to military use during World War I[720], recent technological advancements have expanded their applications in sectors such as parcel delivery[721], imagery capture[722], mapping[723], construction oversight[724], law enforcement[725], and search and rescue[726]. They have become affordable and user-friendly, appealing to hobbyists and professionals alike[727]. Yet, these advancements have also intensified concerns regarding privacy invasion, a recognized issue by scholars[728].

Regulations governing drone use were enacted by the EU in 2019[729], and

---

717 Luke A. Stewart, „The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review", *Information Technology & Innovation Foundation,* (2010): 2.

718 *Ibid.,* 2.

719 „Industry Leading Drone Market Analysis 2022-2030 | Droneii", 2022 m. rugsėjo 20 d., https://droneii.com/drone-market-analysis-2022-2030.

720 John Sifton, „A Brief History of Drones", *The Nation,* 2012 m. vasario 27 d., žiūrėta 2016-02-08. Plačiau žr. http://www.thenation.com/article/brief-history-drones/.

721 Insider Intelligence, „Why Amazon, UPS and Even Domino's Is Investing in Drone Delivery Services", *Insider Intelligence,* žiūrėta 2022 m. gruodžio 1 d., https://www.insiderintelligence.com/insights/drone-delivery-services/.

722 Gabby Robles, „How Drones Are Used in Photography and Cinematography - 42West", *42 West, the Adorama Learning Center* (blog), 2021 m. gruodžio 10 d., https://www.adorama.com/alc/drones-in-cinematography-photography/.

723 „Drone Mapping Applications across Industries", *Wingtra,* žiūrėta 2022 m. gruodžio 1 d., https://wingtra.com/drone-mapping-applications/.

724 *BigRentz,* „6 Ways Drones in Construction Are Changing the Industry – BigRentz", https://www.bigrentz.com, 2022 m. vasario 16 d., https://www.bigrentz.com/blog/drones-construction.

725 Gabby Robles, „How Police Departments Are Using Drones - *42West, Adorama", 42 West, the Adorama Learning Center* (blog), 2022 m. birželio 17 d., https://www.adorama.com/alc/police-drones/.

726 Sharifah Mastura Syed Mohd Daud ir kt., „Applications of Drone in Disaster Management: A Scoping Review", *Science & Justice* 62, 1 (2022): 30–42, https://doi.org/10.1016/j.scijus.2021.11.002.

727 Tyler Francke, „Aurora Resident Reports Disturbing Incident of Drone Apparently Spying Through Her Window", 2019 m. kovo 27 d., https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/, https://canbyfirst.com/aurora-resident-reports-disturbing-incident-of-drone-apparently-spying-through-her-window/.

728 See *infra notes,* 23–32.

729 On March 12, 2019, Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and third-country operators of unmanned aircraft systems, C/2019/1821, OJ L 152, June 11, 2019: 1–40 (Regulation (EU) 2019/945); On May 24, 2019, Commission Implementing Regulation (EU) 2019/947 on rules and procedures for the operation of unmanned aircraft, C/2019/3824, OJ L 152, June 11, 2019: 45–71 (Regulation (EU) 2019/947).

the US released similar rules in 2016 for small drones[730]. International organizations published advisory documents in 2020[731]. However, these regulations primarily address safety concerns, neglecting privacy issues. One of the most import legal acts safeguarding privacy in EU is the General Data Protection Regulation (GDPR)[732], but its applicability to the relationship between drone operators and the public remains unclear.

The nebulous applicability of extant laws to drones, the absence of privacy-centered regulations, and the dearth of theoretical frameworks for future drone-related privacy regulations present challenges. These problems could impede both privacy protection and drone technological advancement. Through an exploration of the current legal landscape, synthesis of scholarly ideas, and assessment of possible solutions, this dissertation seeks to propose adaptive resolutions that harmonize legal frameworks and court practices while safeguarding both privacy and technological progress.

The object of this work revolves around the privacy protection measures employed during the enforcement of legal regulations concerning both commercial drones and privacy.

The objective of this work is to comprehensively examine the current legal dynamics surrounding drone usage, privacy protection regulations, and the specialized regulatory framework for drones and to propose enhancements to these areas.

To achieve this overarching goal, the following specific research tasks have been established:

1. Define the origins and conceptual underpinnings of drones, illuminate the historical roots of the right to privacy in both the continental and common law traditions.

2. Uncover the potential threats to the right to privacy stemming from the utilization of drones.

3. Conduct an in-depth analysis of the privacy safeguards provided by the specialized regulatory framework for drones.

4. Investigate the array of privacy protection measures delineated in both legal regulations and scholarly discourse pertaining to privacy in public spaces.

5. Scrutinize the efficacy of privacy protection measures embedded within data protection regulations.

730 Federal Aviation Administration, „Operation and Certification of Small Unmanned Aircraft Systems", FAA– 2015–0150, Federal Register, 81, 124 (2016): 42064–42214.

731 ICAO model UAS regulations part 101 and 102, (2020); ICAO model UAS regulations part 149, (2020); ICAO Advisory Circular (AC) 101-1, (2020); ICAO Advisory Circular (AC) 102-1, (2020); ICAO Advisory Circular (AC) 102-23, (2020); JARUS UAS Operational Categorization (2019).

732 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119/1, 4.5.2016..

6. Develop proposals for the implementation of regulations specifically tailored for drones in the future.

The novelty and significance of this scientific work are apparent in six key aspects.

Firstly, while existing scientific literature acknowledges the threat drones pose to privacy, it lacks in-depth exploration of specific privacy violations. This dissertation, however, not only identifies these threats comprehensively but also fills a critical gap in the scientific discourse. Secondly, there has been a notable absence of research analyzing the extent of privacy protections provided by the specialized regulation of drones. In response, this thesis meticulously examines the special legislation on drones enacted by the EU, US, and international organizations. This analysis serves to determine whether the current privacy protection measures are indeed adequate. Thirdly, the dissertation addresses a significant ambiguity in the realm of privacy protection linked to drone usage in public spaces. While a plethora of scholarly literature on this topic exists, comprehensive studies delving into the intricacies of drones in public areas are scarce. The dissertation's thorough analysis of scientific sources, legal statutes, and court practices relating to privacy in public spaces stands as a valuable contribution. Fourthly, an unexplored dimension is the assessment of privacy protection measures within the EU's data protection regulation concerning drone utilization. The thesis bridges this gap through a rigorous examination of the GDPR, ultimately revealing whether there's a necessity for specialized privacy regulations for emerging technologies like drones. Fifthly, existing Lithuanian scientific literature inadequately addresses the nuanced evolution of the right to privacy and its diverse interpretations across common and continental legal traditions. This deficiency can result in a misinterpretation of privacy concepts and an unintentional disconnect from the continental legal framework, given the dominance of US-authored privacy law articles. By thoroughly scrutinizing the development of privacy concepts across France, Germany, the USA, and Lithuania, this dissertation seeks to bridge this gap and enrich the quality of scholarly discussions on privacy. Lastly, the conclusions drawn in this work are rooted in theories proposed by eminent legal scholars. This lends credibility to the findings and makes the research a reliable foundation for potential legislative initiatives in Lithuania, judicial decisions, and further studies focused on the intricate interplay between drone usage and the right to privacy.

Work structure. The dissertation is structured into an introduction, four chapters, conclusions, and recommendations.

Chapter 1 examines the potential threats to privacy posed by the use of drones through possible privacy violations. The chapter consists of six sections. The first four sections are dedicated to discussing the concept and origins of drones, as well as the concept of privacy and its origins. The fifth section analyzes specific privacy violations that may result from the use of drones. Finally, the sixth section presents the conclusions of the chapter and the author's insights into how drones

differ from other technologies that may infringe on privacy.

Chapter 2 delves into an analysis of specific sources governing drone regulation. This section identifies privacy safeguards embedded within specific drone regulatory sources and dissects the extent of privacy protection each may offer. The first subsection grapples with the thesis's interpretation of regulatory concepts, while the second tackles drone regulatory documents delineating classifications. The third subsection separately dissects privacy protections within drone regulation. The final subsection culminates in chapter conclusions and recommendations.

The aim of Chapter 3 is to analyze the privacy protection measures proposed by scientific literature, legal regulations, and case law related to privacy issues in public spaces. This chapter examines general privacy protection theories and their applicability in the context of drones. The chapter consists of three subsections: the first subsection discusses privacy issues in public spaces; the second subsection analyzes scientific literature on public space privacy and seeks a theoretical foundation for future privacy regulation in public spaces; the third subsection examines ECtHR and Lithuanian case law related to privacy in public spaces, along with an assessment of jurisprudence in the context of drones.

Chapter 4 probes the governance of drone usage under the current EU data protection framework. The first subsection examines the applicability of GDPR when drones are employed. The second segment delves into lawful data collection bases for drones. Subsequently, the third subsection assesses whether GDPR's proposed privacy safeguards suffice to shield privacy from drone usage. The fourth subsection proffers an evaluation of GDPR within the drone context. The fifth subsection discusses the pitfalls of the current consent-based privacy protection model. Finally, the sixth subsection proposes prospective adjustments to privacy regulation.

This structural decision was made deliberately: first, specific privacy protection measures are examined, as they are directly applicable to drone usage and serve as the primary preventive measure. Only then are general privacy regulation models analyzed to assess whether the existing legal framework is sufficient and in what aspects it could be improved based on theoretical principles. This structure allows for a clearer identification of regulatory shortcomings and enables the proposal of well-founded solutions that can be practically implemented within the current legal system.

Conclusions, recommendations, and a comprehensive reference list conclude the dissertation.

A review of previous research. Throughout the dissertation's preparation, no scientific studies have comprehensively addressed its subject matter. Nevertheless, numerous foreign authors have published works on the privacy risks associated with drones, including Paul McBride (2009)[733],

733 Paul McBride, „Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations", *J. Air L. & Com.* 74 (2009): 627.

Ryan Calo (2011)[734], Rachel Finn and David Wright (2012)[735], Uri Volovelsky (2014)[736], Roger Clarke (2014)[737], Des Butler (2014)[738], Margherita Bonetto (2015)[739], Jonathan P. West and James S. Bowman (2016)[740], Rocci Luppicini and Arthur So (2016)[741]. However, it's noteworthy that none of these studies have conducted an in-depth analysis of the various ways in which drones can infringe upon privacy. Regarding privacy protection measures outlined in the new EU drone regulations No. 2019/945 and 2019/947, a brief article authored by Aurelija Pūraitė and Neringa Šilinskė (2020)[742] is available. However, no other scholarly research on this subject was published either within Lithuania or internationally during the dissertation's preparation. Notably, within Lithuania, the author of this dissertation, D. Kiršys (2016)[743], as well as A. Pūraitė, D. Bereikienė and N. Šilinskė (2017)[744], have written about the threats posed by drones. Internationally, a plethora of publications have focused on the topic of the right to privacy. Pertinent to the theoretical aspect, Daniel Solove's studies (2002-2008)[745] concerning the

734 Ryan M. Calo, „The Drone as a Privacy Catalyst", *Stanford Law Review Online* 64 (2011): 29–33.

735 Rachel L. Finn ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 28, 2 (2012): 184–194.

736 Uri Volovelsky, „Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 30, 3 (2014): 306–20, https://doi.org/10.1016/j.clsr.2014.03.008.

737 Roger Clarke, „Understanding the drone epidemic", *Computer Law & Security Review* 30, 3 (2014): 230–246, https://doi.org/10.1016/j.clsr.2014.03.002; Roger Clarke, „The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 30, 3 (2014): 286–305, https://doi.org/10.1016/j.clsr.2014.03.005.

738 Des Butler, „The Dawn of the Age of the Drones: An Australian Privacy Law Perspective", *University of New South Wales Law Journal* 37, 2 (2014): 434–470.

739 Margherita Bonetto ir kt., „Privacy in mini-drone based video surveillance", *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG),* 4 (IEEE, 2015), 1–6.

740 Jonathan P. West ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues", *Public Administration Review* 76, 4 (2016): 649–659.

741 Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy", *Technology in Society* 46, Supplement C (2016): 109–119, https://doi.org/10.1016/j.techsoc.2016.03.003.

742 Aurelija Pūraitė ir Neringa Šilinskė, „Privacy Protection in the New Eu Regulations on the Use of Unmanned Aerial Systems", *Public Security and Public Order,* 24 (2020).

743 Deividas Kiršys, „Ar bepiločio orlaivio skrydžio vykdymas žemės sklypo oro erdvėje nepažeidžia to žemės sklypo savininko nuosavybės teisės?" (Vytautas Magnus University, 2016).

744 Aurelija Pūraitė, Daiva Bereikienė ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania", *Baltic Journal of Law & Politics* 10, 2 (2017): 107–132.

745 Daniel J. Solove, „Conceptualizing Privacy", California Law Review 90, 4 (2002): 1087–1156; Daniel J. Solove, „Understanding privacy", 2008; Daniel J. Solove, „I've got nothing to hide and other misunderstandings of privacy", San Diego L. Rev. 44 (2007): 745; Daniel J. Solove, „A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154, 3 (2006): 477–564; Daniel J. Solove, „Introduction: Privacy self-management and the consent dilemma", Harv. L. Rev. 126 (2012): 1880.

right to private life hold great relevance. Works by R. Finn et al. (2013)[746] also merit mention. While the historical development of privacy across the Atlantic has not been thoroughly analyzed within Lithuania, numerous foreign authors have delved into this subject. Noteworthy contributions include those by James Q. Whitman (2003)[747], Anupam Chander, Margot E. Kaminski and William McGeveran (2020)[748], Paul Schwartz (2012)[749], Oliver Diggelmann and Maria Nicole Cleis (2014)[750], Raymond Wacks (1980)[751], Richard A. Posner (1981)[752], André Bertrand (1999)[753], Rudolf von Jhering (1869)[754]. Within Lithuania, Gediminas Bučiūnas (2010, 2015)[755], Kamilė Mekšriūnaitė (2019)[756] and Toma Razmaitė (2014)[757] have explored the right to private life in contexts tangentially related to drone usage. Regarding privacy in the public space, Lithuania has yet to witness scientific publications on this matter. Consequently, foreign scholars' works, albeit not focused specifically on drone usage, have been scrutinized for insights. Such scholars include Helen Nissenbaum (1998)[758], Joel R. Reidenberg (2014)[759], and M.E. Kaminski (2015)[760]. In terms of GDPR's implications in the drone context, both Lithuanian and foreign researchers have not extensively delved into this aspect. However, GDPR has been explored in relation to other facets that could potentially intersect with drone use, exemplified by research by

746 Rachel L. Finn, David Wright ir Michael Friedewald, „Seven types of privacy", *European data protection: coming of age* (Springer, 2013), 3–32.
747 James Q. Whitman, „The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal* 113, 6 (2004): 1151–1222.
748 Anupam Chander, Margot E. Kaminski ir William McGeveran, „Catalyzing Privacy Law", *Minnesota Law Review* 105, 4 (2021): 1733–1802.
749 Paul M. Schwartz, „The EU-US privacy collision: a turn to institutions and procedures", *Harv. L. Rev.* 126 (2012): 1966.
750 Oliver Diggelmann ir Maria Nicole Cleis, „How the Right to Privacy Became a Human Right", *Human Rights Law Review* 14, 3 (2014 m. rugsėjo 1 d.): 441–458, https://doi.org/10.1093/hrlr/ngu014.
751 Raymond Wacks, *The protection of privacy* (Sweet & Maxwell, 1980).
752 Richard A. Posner, „The economics of privacy", *The American economic review* 71, 2 (1981): 405–409.
753 André Bertrand, *Droit à la vie privée et droit à l'image* (Lexis Nexis, 1999).
754 Rudolf von Jhering, *Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung,* t. 2 (Breitkopf und Härtel, 1869).
755 Gediminas Bučiūnas, „Vaizdo registratoriai ir asmens privatumas", *Mokslo taikomieji tyrimai Lietuvos kolegijose* 1, 11 (2015): 64–68; Gediminas Bučiūnas, „Sekimas ir asmens privatumas: kur riba?" (Vilnius: Mykolo Romerio universitetas, 2010).
756 Kamilė Mekšriūnaitė, „Valstybės institucijų vykdomo asmenų sekimo problematika teisės į privataus gyvenimo apsaugą atžvilgiu" (Vilnius: Mykolo Romerio universitetas, 2019).
757 Toma Razmaitė, „*Google Street View* atvejis: teisės į privatumą ir technologijų plėtros santykis" (Vilnius: Mykolo Romerio universitetas, 2014).
758 Helen Nissenbaum, „Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy* 17, 5/6 (199): 559–596.
759 Joel R. Reidenberg, „Privacy in Public", *University of Miami Law Review* 69, 1 (2014): 141–160.
760 Margot E. Kaminski, „Regulating Real-World Surveillance", *Washington Law Review* 90, 3 (2015): 1113–1166.

Aurimas Šidlauskas (2019)[761], Mamoonas Asghar et al. (2019)[762], Jane Andrew and Max Baker (2021)[763], Yola Georgiadou, Rolf A. de By and Ourania Kounadi (2019)[764], as well as Gerald Spindler and Philipp Schmechel (2016)[765], Piero A. Bonatti and Sabrina Kirrane (2019)[766].

In sum, neither within Lithuania nor internationally have any studies emerged that comprehensively address the threat to privacy stemming from drone usage. Scholarly articles precisely defining and analyzing privacy protections within drone-specific legislation are also absent. Similarly, there is a lack of scholarly publications analyzing the application of GDPR to drones.

Research Methodology

This dissertation employs a combination of research methods to facilitate comprehensive analysis.

Document Analysis Method: This approach was employed to identify and comprehend primary information sources. The analyzed data sources are grouped into four principal categories. First, scholarly works by Lithuanian and international researchers that elaborate on drone utilization. Second, theoretical research papers concerning the right to privacy. Third, research papers, legal precedents, and regulations pertinent to privacy within the public domain. Fourth, scientific literature, legal statutes, and case law related to EU data protection regulation.

Data collection utilized resources from Mykolas Romeris University library, subscription databases, foreign library archives, university databases, and reputable electronic publications. Instances from ECtHR and the Supreme Court of Lithuania were located through platforms such as "Infolex," "eTeismai," "Liteko," and the "HUDOC" database. Legal enactments from Lithuania and other nations were sourced from the official websites of respective legislative authorities and their publications.

Historical Method: This methodology is employed to elucidate the historical underpinnings that have culminated in the contemporary utilization of drones.

761 Aurimas Šidlauskas, „Video Surveillance and the GDPR", 2019.

762 Mamoona Asghar ir kt., „Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective", IEEE Access 7 (2019 m. rugpjūčio 9 d.): 111709–111726, https://doi.org/10.1109/ACCESS.2019.2934226.

763 Jane Andrew ir Max Baker, „The general data protection regulation in the age of surveillance capitalism", *Journal of Business Ethics* 168, 3 (2021): 565–578.

764 Yola Georgiadou, Rolf A. de By ir Ourania Kounadi, „Location Privacy in the Wake of the GDPR", *ISPRS International Journal of Geo-Information* 8, 3 (2019): 157, https://doi.org/10.3390/ijgi8030157.

765 Gerald Spindler ir Philipp Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7, 2 (2016): [i]-177.

766 Piero A. Bonatti ir Sabrina Kirrane, „Big Data and Analytics in the Age of the GDPR", *2019 IEEE International Congress on Big Data (BigDataCongress)* (2019 IEEE International Congress on Big Data *(BigData Congress),* Milan, Italy: IEEE, 2019), 7–16, https://doi.org/10.1109/BigDataCongress.2019.00015.

It is also utilized to trace the origins of the right to privacy in countries like France, Germany, the United States, and Lithuania.

Systematic Analysis Method: Employing this method, the dissertation systematically scrutinizes both general privacy considerations and the specific regulations pertaining to drones. This systematic exploration reveals the intricate connection between drone usage and privacy.

Comparative Analysis: Utilized to ascertain divergent perceptions of privacy across legal systems, this approach delves into the provisions of specialized legal documents governing drones issued by various organizations. It also contrasts theories of privacy within public spaces.

Analytical Critical Method: This method is employed to address the deficiencies apparent in specialized drone regulations instituted by diverse organizations, as well as within ECtHR, Lithuanian judicial practices, and EU data protection legislation. It is also utilized to tackle implementation challenges and shortfalls in legal solutions proposed within scholarly literature.

Defensive Statements:

1. Drones possess unique characteristics not found in any previously used technologies that could infringe on privacy. These characteristics contribute to the blurring of boundaries between the virtual and real worlds, allow for widespread use, enable intensive surveillance from various angles, have the potential to be weaponized, and are difficult to detect. Consequently, the EU, US, and international special regulations for drones, which are primarily focused on ensuring security and are based on the self-management privacy paradigm, are insufficient to adequately protect privacy. This creates the need for improvements in special regulatory frameworks.

2. The current legal framework for privacy protection is based on the self-management privacy paradigm. For more effective privacy protection in the context of drone use, future regulatory developments should adopt the paternalistic boundary management theory.

1. THE THREAT TO PRIVACY POSED BY DRONES

Drones pose a threat to privacy – this is acknowledged by many researchers. However, in their efforts to illustrate the ways in which the right to privacy is violated, scholars tend to limit themselves to one or a few examples. In other words, while the scientific literature recognizes the existence of a threat, specific privacy violations resulting from the use of drones are not examined in detail. This leads to another issue: without identifying actual privacy violations, it becomes difficult to determine what measures should be taken to prevent privacy breaches in the future. This chapter of the dissertation aims to identify the specific threats that drones pose to privacy. However, before delving into the legal issues related to drones and privacy, it is

worth briefly discussing the origins of the technology now known as drones, reviewing the various terms used to describe them in different sources, and understanding the historical development of the modern concept of privacy.

This chapter, consisting of six subsections, addresses the first and second research objectives of the dissertation. The first subsection discusses the concept of drones, while the second analyzes their historical and technological origins. The third subsection examines the complexities of the privacy concept, and the fourth explores the historical roots of privacy. The fifth subsection then moves on to specific privacy violations that may arise from the commercial use of drones. Finally, the chapter concludes with the sixth subsection, which summarizes how drones differ from other technologies that can infringe on privacy. This analysis will serve as the foundation for the subsequent chapters of the dissertation, which will evaluate the legal regulation of drones and privacy.

1.1. The Concept of a Drone

The term "drone" in a broad sense refers to both aerial unmanned vehicles and ground-based unmanned systems. Both types of drones share a common feature: they can perform tasks that would be difficult or even impossible for humans. Despite their wide range of applications, the term "drone" has become widely associated with aerial systems, a preference seen not only among journalists but also among researchers and government officials. However, legal texts more frequently use alternative terms for flying drones that more precisely describe their ability to fly. For example, U.S. institutions commonly use the term *Unmanned Aerial Systems (UAS),* while the EU and ICAO use *Unmanned Aircraft Systems (UAS).* Different jurisdictions define drones differently. However, considering that a drone consists of multiple components necessary for flight and for the sake of clarity, this dissertation refers to the entire unmanned aerial system (UAS) simply as a drone.

1.2. The Origins of Drones

1.2.1. Historical Origins

Unmanned aerial vehicles (UAVs) are one of the most advanced technologies, with development spanning over 100 years. It can be argued that the first drones were unmanned air balloons used for bombing missions during World War I. Later, throughout World War II and the Cold War, they were not only utilized in the military industry but also improved – from aerial torpedoes to radio-controlled missiles and sophisticated fighter jets. The history of commercial drones began only a decade ago, but their technology is not entirely new. They consist of numerous components that have evolved at different stages of modern society's development. The technological origins of drones should be examined in more detail in the next subsection.

I.2.2. Technological Origins

Although legislators have created legal regulations to address the changes brought about by previous technologies, the continuous development of technology often requires the creation of new rules. When new technologies emerge in the market, uncertainty arises, and many situations must be assessed using outdated regulations or intuition. However, just as new technologies are linked to their predecessors, legal acts regulating earlier technologies are also connected to the regulations of even older technologies. In other words, newly developed legal regulations are based on previously adopted legal decisions and seek similarities in existing laws. Similarly, the foundations of drone regulation can be explored by examining the legal framework of related technologies.

According to Adam Rothstein, drones are similar to three technologies: automobiles, aircraft, and robots. Roger Clarke, on the other hand, compares them to computers, telecommunications, robots, and cyborgs. The author of this dissertation believes that the issue at hand is related to privacy protection, with the greatest threat posed by drone components capable of collecting personal data, insufficiently secured data transmission lines, and unreliable software processing personal data.

From a privacy perspective, drones are most similar to three technologies:

1. *Video cameras* – like drones, they can collect large amounts of personal data in the real world.

2. *Computers* – both use software to analyze collected data and convert it into a standardized format.

3. *Telecommunications* – like drones, they enable data transmission from one location to another.

I.3. The Concept of Privacy

Despite its widespread recognition, there is no universally agreed-upon concept of privacy. It may be difficult to define the right to privacy because it is constantly evolving. For example, some researchers believe that the perception of privacy is shaped by two variables: a social factor, which depends on society, and a technological factor, which is influenced by technological development. The social factor consists of two aspects. The first is related to the political structure of a society – whether it is a democratic country characterized by a free market, freedom of speech, and relatively little government interference in individuals' private affairs, or, conversely, a communist state where the government partially or fully controls the market, censors the press, and conducts large-scale surveillance of citizens. It is likely that the perception of privacy among people living in liberal societies differs significantly from that of those in collective socialist states. For example, in

Lithuania between 1940 and 1990, under the socialist regime, individuals could not expect any privacy from the state.

The second aspect is a country's legal tradition and its influence on social norms, specifically how society defines private life. This is shaped by both the country's history and the development of its legal system. Although most European countries and the United States are based on liberal democracy, people in different nations perceive privacy differently. For instance, in some continental European countries, nudists in public city parks may be a common sight, whereas in the U.S., this would be considered taboo. Similarly, people in continental Europe often struggle to understand the American culture of celebrity chasing and paparazzi.

To comprehend these differences in perception, it is necessary to examine the historical development of the right to private life. Since this dissertation relies on legal documents from both the U.S. and Europe, before analyzing drone-related privacy regulations, it is worth exploring the circumstances under which the concept of privacy was created – one that is referred to as "privacy" on both sides of the Atlantic, yet understood differently.

l.4. Historical Origins of Privacy

This section examines how the concept of privacy was formed and developed in different legal traditions – France, Germany, the United States, and Lithuania. The analysis of historical contexts helps to better understand why continental and common law tradition countries regulate privacy protection differently today.

1.4.1. Origins of Privacy in France

Privacy protection in France is linked to the 1791 Constitution, which, in addition to freedom of the press, also established the protection of honor and private life. In the mid-19th century, after censorship was abolished, courts began addressing disputes related to the "right to one's image." One of the first notable cases was that of Alexandre Dumas père, in which the court ruled that an individual's privacy takes precedence over property rights to photographs. This legal practice established the principle that privacy is a non-transferable personal right inherently tied to an individual's honor.

1.4.2. Origins of Privacy in Germany

In Germany, the right to private life is also linked to honor, but German theorists based its origins on the Roman law concept of *iniuria* and Hegelian philosophy. By the late 19th century, the doctrine of *Persönlichkeitsrecht* (personality

rights) had emerged, encompassing non-economic interests such as name, image, and reputation. These ideas were incorporated into the German Civil Code, which came into effect in 1900, as well as later constitutional provisions that protect personal freedom and honor as fundamental human values.

1.4.3. Origins of Privacy in the United States

In the United States, the right to privacy originates from the Fourth Amendment of the Constitution, which protects individuals from government intrusion into their homes. In the 1886 case *Boyd v. United States,* this protection was expanded to encompass general "privacy of life." In 1890, Samuel Warren and Louis Brandeis proposed a European-style right to privacy, but it did not develop in the U.S. in the same way as in continental Europe. In the U.S., privacy is more often understood as freedom from government actions, while an individual's image is considered a property right that can be sold without restrictions.

1.4.4. Modern Perception of Privacy on Different Sides of the Atlantic

In Europe, privacy is considered part of honor and dignity, with the greatest threat coming from the media, whereas in the United States, it is viewed as freedom from government interference. In Europe, privacy is often protected through the institution of non-material rights (such as the right to a name, image, and dignity), while in the U.S., the emphasis is on the proprietary aspect of one's image and strong freedom of expression. However, there are shared principles, such as the inviolability of the home, but overall, the continental and common law traditions differ significantly.

1.4.5. Privacy in Lithuania

The interwar Lithuanian constitutions ensured the confidentiality of correspondence and the inviolability of the home, but actual privacy protection was limited, especially during the Soviet era. After regaining independence, the Constitution and the Civil Code established a Western-style concept of privacy, incorporating elements from both continental and American legal traditions. In Lithuania, privacy is protected as a non-material value (including the right to one's image, honor, and dignity), while also recognizing the inviolability of an individual's home. The Civil Code and other laws provide various legal protections, including administrative and criminal liability for privacy violations, emphasizing a high level of privacy protection.

1.5. Privacy Violations That May Be Caused by the Use of Drones

To reveal the theoretical privacy threats posed by the use of small drones, it is useful to examine the classifications of the right to privacy discussed in academic literature. Legal doctrine distinguishes two main approaches to classifying privacy: by the values being violated or by the types of violations. The first approach was developed by European scholars, while the second was established by researchers in the United States. In continental Europe, privacy has been categorized into seven value-based categories by R. Finn, D. Wright, and M. Friedewald. Meanwhile, in U.S. law, one of the most comprehensive classifications of privacy violations was created by D. J. Solove. This dissertation follows Solove's classification. Of course, drones do not cause every type of violation listed in the classification, so more attention is given to those threats most closely associated with drone use – namely, surveillance, aggregation, identification, insecurity, and exposure.

1.5.1. Surveillance

Drones can capture images, sound, and other data, enabling continuous surveillance of individuals. This can be carried out not only by the state but also by private entities, and the vast amounts of collected data can be used in the future. Constant surveillance leads to a "panoptic effect," where people feel watched even without actual monitoring, restricting their freedom, self-expression, and encouraging conformity. Even in public spaces, individuals can expect a certain level of privacy, but the expansion of drones facilitates individual tracking, reduces surveillance costs, and increases the ability to gather information on every person.

1.5.2. Aggregation

Aggregation is the processing of already collected information, where different data fragments are combined into a unified whole. The data collected by drones is later analyzed by advanced programs capable of detecting patterns in individuals' behavior. In the world of big data, everyone is monitored, not just suspects, leading to greater concentration of power in the hands of those who control this information. Aggregation can result in incorrect conclusions if the data is inaccurate or the algorithms are biased, which can have serious consequences for individuals' opportunities (e.g., employment, obtaining a loan).

1.5.3. Identification

Identification is the linking of specific data to a particular individual. While this facilitates the search for criminals, it also increases the risk of misuse of personal data, fosters bias, and limits anonymity. Facial recognition technologies combined with drones enable real-time tracking of individuals, strengthening control by the state or other entities. Such a system can be used for totalitarian purposes, where citizens cannot escape constant surveillance and identification.

1.5.4. Insecurity

Drones expand the scope of collected data, making it an attractive target for cybercriminals. Hacking into databases or the drone itself can allow attackers to take control, conduct espionage, alter crime scenes, or launch bot attacks. Even large corporations are not fully protected from cyber incidents, making the inability of data controllers to ensure security a major privacy violation – especially as drones create even more opportunities to collect and transmit sensitive information.

1.5.5. Exposure

Exposure refers to the public revelation of an individual's vulnerable or private physical and emotional aspects, which can lead to shame, humiliation, or even social stigmatization. Drones make it easier to capture individuals in private spaces (e.g., at home, in their yard), where they expect to be alone. Public disclosure of such images can have serious psychological consequences and serve as a means of blackmail. Due to the accessibility of drones, such privacy violations are becoming more frequent and harder to control.

1.6. Chapter Conclusions: How Do Drones Differ from Other Privacy-Compromising Technologies?

Drones can fundamentally change the scale and intensity of privacy violations. They not only merge the virtual and real worlds but can also operate discreetly, conduct continuous surveillance of individuals, and serve as tools of physical intervention. This technological combination enables extensive, intense, and multi-angled information collection, meaning that insufficiently regulated drone use could significantly impact human behavior and even the democratic order.

The main reasons why drones differ from other surveillance technologies:

Blurring the boundaries between the virtual and real worlds. Drones can capture detailed real-time images and sounds while integrating them with data collected in virtual environments, creating an exceptionally comprehensive picture of an individual's behavior, interests, and daily life that purely virtual tools could not provide.

Widespread use. Drones are relatively inexpensive, small, and easily adaptable, meaning their numbers could increase significantly in the near future. Governmental and private organizations with access to data infrastructure will be able to utilize drone-collected information even more effectively.

Intensity of surveillance. Unlike stationary CCTV cameras or user-dependent smartphones, drones can continuously and closely track individuals, capturing images and sounds that can later be analyzed and stored indefinitely.

Diverse surveillance angles. Drones can overcome physical obstacles, fly at various heights and angles, and capture footage from difficult-to-reach locations, providing a much more detailed and comprehensive view than fixed cameras or other limited-range devices.

Potential weaponization. Drones can be equipped not only with surveillance equipment but also with actual weapons, loudspeakers, or hacking tools. This intensifies the "chilling effect," where individuals, knowing they are being watched, may fear direct physical coercion.

Stealth. Drones can be designed to resemble birds, insects, or be extremely small, enabling covert surveillance where individuals are unaware they are being monitored or why their data is being collected.

Comparison of drones with other technologies:

Smartphones collect vast amounts of personal data but primarily in the virtual space and usually with the user's knowledge. Drones, however, can observe the real world without consent or interaction.

CCTV cameras are stationary and capture only a fixed location, whereas drones can move and collect information across a much broader area.

Social networks store data in virtual environments but cannot monitor daily physical activities in detail. Drones, on the other hand, track real-time behavior and locations.

Smart home assistants primarily function in fixed locations and collect voice data, but they lack mobility and the ability to record the user's surroundings.

Internet cookies are limited to the virtual world and web browsers, whereas drones can collect both online and real-life data, expanding the scope of potential manipulation.

Conclusion: due to their mobility, extensive reach, ability to observe from multiple angles, and potential for weaponization, drones create unprecedented conditions for information gathering and individual control. Compared to other surveillance technologies, their unique capabilities pose a significant privacy threat, necessitating proper legal regulation to ensure both public safety and fundamental personal freedoms.

2. PRIVACY PROTECTION PROVIDED BY SPECIALIZED DRONE REGULATIONS

The analysis of the historical origins of privacy has revealed how differently the right to privacy is understood, while the classification of privacy violations (Figure 1) has highlighted the risks associated with drone use. One of the key characteristics of drones that may shift the concept of privacy is their ability to conduct surveillance without the knowledge of the observed individual (stealth). As a result, those being monitored may not even suspect that someone is using a drone to violate their privacy. This poses a challenge when seeking legal remedies for such violations, such as the right to take legal action. For traditional civil liability principles to be effective, special regulations are needed to limit drone stealth to a level where the affected party can detect privacy violations and provide evidence that they occurred. Such measures should have a preventive function – the fewer opportunities there are for covert surveillance, the fewer privacy violations will take place.

This dissertation chapter analyzes preventive privacy protection measures outlined in specialized drone regulations and sources, aiming to preemptively address privacy violations. The study of privacy violations examines regulatory documents from ICAO, JARUS, the EU, and the U.S. ICAO and JARUS were chosen due to their significance in international drone regulation – their technical standards often serve as a foundation for national regulations, ensuring a unified approach to drone use across different countries. These standards help establish common guidelines, facilitating international drone operations and improving regulatory harmonization. The U.S. and EU were selected due to their significant legal and cultural differences: U.S. law prioritizes technological innovation and market freedom, whereas the EU emphasizes strict privacy protection and the role of government regulation. This selection aims to highlight both the strengths and weaknesses of different regulatory models.

This chapter fulfills the third objective of the dissertation. The first subsection discusses possible approaches to legal regulation, helping the reader better understand the concept of regulation used in the dissertation and the legal authority of each source analyzed in this section. The second subsection summarizes the

sources examined in the study and the drone classifications used in them. The third subsection identifies privacy protection measures established by specialized drone regulations that could hypothetically reduce the likelihood of privacy violations and discusses the extent to which each measure could realistically protect privacy.

2.1. The Concept of *Regulation*

Legal regulation is one of the forms of social regulation; however, in this study, regulation is understood more broadly – not only as the establishment of legal norms but also as various other measures, including soft law. According to EU practice, regulatory interventions can take different forms, ranging from formal legislation to information dissemination, self-regulation, co-regulation, standardization, and market-based measures.

Drone regulation is still evolving, and traditional legal mechanisms are not yet fully defined. Therefore, a broader understanding of regulation is proposed, encompassing organizational initiatives and their proposed privacy protection measures.

2.2. Specialized Drone Regulation

2.2.1. Sources

At the international level, the main organizations shaping drone regulation are ICAO and JARUS. ICAO, a United Nations agency, develops model regulations that member states can adapt to their national frameworks. JARUS, an international expert group, provides recommendations on drone safety and certification.

In Europe, the key institutions are the European Commission, EASA, and SESAR JU, which aim to establish an automated drone traffic management system known as "U-space." EU regulations, enshrined in the General Aviation Regulation and other legal acts, ensure not only safety but also privacy and data protection.

In the United States, drone regulation is overseen by the FAA, which has issued rules defining drone usage and certification requirements. However, direct privacy regulation is not included – current policies rely on general guidelines.

Comparing different jurisdictions, the EU incorporates privacy protection into formal regulations, the U.S. relies on general guidelines, and ICAO and JARUS do not directly regulate privacy issues. Despite these differences, even indirect regulatory measures can contribute to privacy protection. This section examines the regulatory sources of each institution and their impact on drone-related privacy concerns.

2.2.2. Drone Classifications

Drone classifications vary across jurisdictions. The EU has the most detailed system, categorizing drones by risk level into open, specific, and certified categories. The open category is further divided into subcategories A1, A2, and A3, while classification by weight includes classes C0 to C4.

JARUS follows a similar system to the EU but differs in its weight-based classification of drones. ICAO, on the other hand, applies only two categories – open (<25 kg) and specific (>25 kg) – without further subcategories.

The U.S. regulatory framework does not classify drones by weight or risk level but instead distinguishes between recreational and commercial operations. Currently, U.S. regulations do not cover drones weighing more than 25 kg.

From a privacy risk perspective, the greatest threats come from small, low-noise, and hard-to-detect drones. Most jurisdictions define small drones as those weighing up to 25 kg. While larger drones do not pose a direct privacy threat, regulatory measures applied to them could also be adapted for smaller drones to strengthen privacy protection.

2.3. Privacy Protection Measures in Specialized Drone Regulations

The subsection is described in the dissertation.

2.4. Chapter Conclusions and Recommendations

Summarizing the analysis of specialized drone regulation sources, the following conclusions can be drawn regarding each hypothetical privacy protection measure:

The requirement to maintain a distance, as outlined in current regulations, would not be a sufficient privacy protection measure. Current drone regulations address this obligation in three ways: 1) ICAO and the EU specify exact distances that drones must maintain from third parties, 2) JARUS establishes a general obligation to maintain a safe distance, and 3) the U.S. does not specify a particular distance. The author of this dissertation believes that effective regulation should define a specific distance, but even this would only be a temporary and indirect privacy protection measure, particularly against drones with low-resolution cameras and basic microphones. Determining a precise distance to protect privacy from drones would require assessing each situation individually, significantly increasing time costs. Thus, this measure is ineffective in mitigating privacy threats posed by drone use.

The requirement to inform (obtain consent), as presented in current regulations, would not be an effective means of protecting privacy. The primary issue is the complexity of informing individuals (to obtain consent). Drone flights cannot be equated to internet browsing, where the consent procedure is widely used. Online, consent can be requested before a person accesses a website, and if they refuse, the website can either block access or simply refrain from collecting data. However, in the real world, it is difficult to imagine a mechanism that would automatically inform everyone in the drone's flight area and, if they object, prevent data collection. ICAO addresses this issue by significantly relaxing consent requirements, allowing for implied consent – creating opportunities for drone operators to exploit regulatory loopholes. The EU has strict and detailed consent requirements, but they are practically unenforceable in crowded areas. The U.S. takes the stance that there is currently no need to formally require notification and consent from bystanders; it is only recommended and left to the discretion of the drone operator.

The registration requirement is one of the most important privacy protection measures, ensuring individuals can exercise their right to seek legal remedies. However, not all jurisdictions analyzed effectively enforce this requirement. Exemptions based solely on drone weight (JARUS) allow manufacturers to produce drones that evade legal oversight but can still violate privacy. Registering all drones (ICAO, U.S.) is preferable to weight-based exemptions but is not the optimal solution, as it may unnecessarily restrict toy drone use. A more effective approach, as seen in EU regulations, is to consider additional conditions alongside weight limitations – for example, exempting drones only if they cannot capture personal data or are classified as toys. This model could serve as a best practice for other legal systems.

The requirement to retain recorded data could contribute to privacy protection, but current specialized drone regulations define data retention obligations too narrowly for it to be an effective measure. A higher level of protection could be ensured if more data were retained, but only under the following conditions: 1) data is stored solely within the drone and not accessible online, 2) third-party access is allowed only upon request from an authorized authority (such as a court or law enforcement), and 3) data has a clearly defined retention period.

Qualification requirements for drone pilots are specified in only two of the analyzed jurisdictions (JARUS and the EU). Requirements such as including a user manual with drones, conducting informational campaigns, mandating training for operators of larger drones, and imposing penalties for non-compliance could be effective privacy protection measures, but their implementation should not be merely formal. User manuals and mandatory training should provide memorable, targeted, and practical information that genuinely contributes to privacy protection.

Informational campaigns should be designed for specific target audiences with engaging messages that encourage action and clearly specify necessary changes.

The requirement to conduct risk assessments under current specialized drone regulations is unlikely to provide adequate privacy protection, as operators are not required to assess privacy risks associated with their flights. However, risk assessments could be an effective privacy protection tool if drone operators were required to evaluate potential privacy harm before certain flights. This approach aligns with EU data protection laws.

Remote identification requirements are most comprehensively regulated by the EU and the U.S., with similar rules in both jurisdictions. Under both EU and U.S. regulations, drones must transmit basic identification data via local radio signals, linking the drone (and its operator) to a centralized registry. However, both regulatory systems have weaknesses. The EU's exception for small drones under 250g means that potentially privacy-violating drones could remain unidentifiable to affected individuals. The author of this dissertation proposes addressing this issue by making remote identification mandatory based on a drone's ability to collect personal data or simply tying it to the registration requirement. In the U.S., potential abuse may arise due to "sandbox" exemptions, creating the same issue as in the EU – small drones capable of violating privacy may not be identifiable to affected individuals. However, the risk of abuse is somewhat mitigated by strict FAA penalties for non-compliance. The dissertation author suggests a technological solution: drone manufacturers could be required to pre-program drones to prevent takeoff in restricted areas without authorization.

Both the U.S. and EU regulations have a fundamental flaw that weakens **remote identification** as a privacy protection measure. Currently, flight identification data is only transmitted locally (via radio signals), making it difficult to detect violations when drones are used for covert surveillance. A potential solution would be to require transmission of identification data not only via radio signals but also over the internet to a central government authority. However, based on the recent approach of the U.S. FAA, implementing this proposal may be challenging due to the underdeveloped state of remote identification technology.

Geofencing (geographical restrictions) has significant potential as a privacy-enhancing technology in the drone sector. In the future, it could address many privacy threats posed by drones in private spaces (land properties, residential areas). However, current geofencing regulations and technology remain underdeveloped. To encourage the development of this innovation, the author of this dissertation suggests that governments adopt less intrusive measures that promote its application in protecting privacy from drone-related threats.

Ensuring the security of data transmission channels is crucial for establishing sustainable drone regulations that prioritize privacy protection. Although advancements in data encryption technologies depend on IT and engineering efforts, legal regulations could guide the direction of this innovation. Countries should focus not only on ensuring continuous data transmission but also on its security.

The requirement for drones to be equipped with lights is one of the easiest, cheapest, and most effective privacy protection measures. Therefore, this requirement should apply to all drones capable of capturing personal data, regardless of whether the flight occurs during the day or night. Of course, the drone's light source should be of sufficient intensity to be visible from a distance effective for privacy protection and noticeable even on a sunny day.

As demonstrated by the analysis of specialized drone regulation sources, the hypothesis proposed at the beginning of this chapter has been confirmed – all discussed measures could, in one way or another, help prevent privacy violations. However, many of these measures do not currently provide effective privacy protection because the regulations governing them have shortcomings, some are not yet fully implemented, or their implementation is challenging. Despite these regulatory gaps, the foundations for reducing drone stealth have been established, and it is expected that as privacy-enhancing technologies advance, the regulation of preventive privacy protection measures will also improve.

3. DRONES AND PRIVACY IN PUBLIC SPACES

After a detailed discussion of the privacy protection measures provided by specialized drone regulations, it is important to analyze the solutions offered by general privacy regulation. As previously mentioned, one of the key privacy violations that can result from the use of small drones is surveillance. In the context of drones, this type of violation is particularly significant, as it enables opportunistic and pervasive data collection, which in turn leads to other privacy infringements. This type of data collection is easiest and most relevant in public spaces, making it necessary to explore privacy risks stemming from the increasing use of drones through one of the fundamental limitations on the right to private life – the collection of data in public places. This dissertation chapter addresses this issue and fulfills the fourth research objective.

The chapter consists of four subsections. The first subsection examines the challenges of privacy in public spaces. The second explores theoretical approaches to privacy regulation in public spaces as discussed in academic discourse. The third subsection analyzes the case law of the European Court of Human Rights (ECtHR)

and Lithuanian courts concerning privacy in public spaces, discussing how jurisprudential principles could be applied to drone-related cases. The final subsection summarizes the privacy protection solutions examined in this chapter.

Research Limitations and Scope

In conducting this research, it was necessary to establish boundaries and select analytical priorities to maintain the dissertation's focus and ensure the relevance of the findings. One such methodological decision was to limit the scope of the jurisprudence analyzed and concentrate on legal systems directly related to Lithuanian case law and potential future regulatory frameworks.

Since the second part of the dissertation extensively examined both EU and U.S. specialized drone regulations, it would be systematic to analyze U.S. case law on privacy in public spaces in this chapter as well. However, it was deliberately excluded because U.S. privacy law follows a fundamentally different methodology from the European legal system, and the legal interpretation standards developed in the U.S. are difficult to directly apply to Lithuanian jurisprudence.

In U.S. case law, a binary concept of privacy prevails, with a strict distinction between public and private spaces – privacy protections apply almost exclusively in private spaces, and expectations of privacy in public places are generally very limited. This approach differs significantly from the interpretation of Article 8 of the European Convention on Human Rights (ECHR) in ECtHR case law, where it is recognized that individuals may expect a certain level of privacy even in public spaces, especially when surveillance is systematic, prolonged, or conducted using advanced technologies. Lithuanian case law relies more heavily on ECtHR-established privacy standards, so an analysis of U.S. jurisprudence would not add significant value to this study.

To maintain analytical consistency and avoid excessive information, a similar decision was made to select only cases that best illustrate key legal issues related to privacy in public spaces. Although a broader range of case law was reviewed, including decisions from the Supreme Administrative Court of Lithuania (LVAT), cases from this court are not discussed in this dissertation chapter. This decision was made because no cases were identified in which the factual circumstances or legal arguments directly addressed privacy protection issues in public spaces in the context of drone use. To avoid redundant information and maintain the study's focus, this jurisprudence is not analyzed in detail.

Since the primary focus was on privacy protection in the context of drone use, priority was given to an in-depth case analysis rather than a quantitative overview. This methodological choice not only helps to clearly identify key jurisprudential principles but also allows for the formulation of well-founded recommendations for future judicial interpretations and legislative processes in the Lithuanian legal system.

3.1. The Issue of Privacy in Public Spaces

While privacy in private spaces is clearly defined, its boundaries in public spaces become more complex. Drones can alter people's behavior and reduce their sense of freedom, even when they are not physically noticeable.

A hypothetical scenario illustrates this issue: a consulting firm uses insect-sized drones to monitor individuals, track their behavior and conversations in public spaces, and integrate the collected data with online databases. Although the surveillance occurs in public, people still do not want their data to be secretly collected.

The author of this dissertation argues that a complete ban on drone flights is not a suitable solution, but clear privacy boundaries are necessary. This issue could be left to the courts and the market to decide, but a theoretical foundation would be required. U.S. scholars H. Nissenbaum, J. Reidenberg, and M. E. Kaminski propose different models for regulating privacy in public spaces.

3.2. The Theoretical Basis for Regulating Privacy in Public Spaces
3.2.1. The Contextual Integrity Theory

H. Nissenbaum criticizes traditional privacy theory, which is based on the distinction between public and private spaces, arguing that the key factor is not the space itself but the context in which data is collected. She emphasizes that even publicly disclosed information should not be used without an individual's consent if it was shared within a specific context.

F. Schoeman illustrates this issue with an example of a gay rights activist who openly expresses his views in one city but wishes to keep this information private in another. This demonstrates that information can be sensitive depending on the context in which it is used.

Nissenbaum's theory is often compared to the GDPR's purpose limitation principle, but its application in the context of drones is limited. The theory focuses on the problem of data transfer but does not address the legality of initial data collection. As a result, laws based on this model would regulate data usage rather than its collection, leaving this issue to the courts or leaving it unregulated. This would mean that drones could collect data without clear restrictions, failing to provide sufficient privacy protection.

3.2.2. The Public Significance Filter Theory

J. Reidenberg proposes that courts use a "public significance filter" instead of the "reasonable expectation of privacy" test when addressing privacy violations. His theory holds that publicly accessible information should still be considered private if it lacks public significance.

He draws on U.S. case law: in Katz, the court recognized that a person has a right to privacy in a phone booth; in Whalen, he disagreed with the ruling that patient data is not private. In Reed, however, he agreed that the names of petition signers have public significance and cannot be considered private.

However, this theory has drawbacks: it provides an unclear framework for privacy regulation, shifting the burden of decision-making to courts; it does not clarify how to distinguish private from public information; and it fails to resolve conflicts between privacy and freedom of expression. Therefore, its application in the context of drones would be limited and would not contribute to more effective privacy protection.

3.2.3. The Boundary Management Theory

M. E. Kaminski argues that people use various strategies to manage their privacy in public spaces – ranging from verbal and non-verbal behavior to the use of environmental objects (e.g., doors, walls). She highlights that privacy boundaries depend on context, but people often rely on established behavioral patterns rather than consciously analyzing each situation.

Technological advancements alter human behavior in public spaces, so lawmakers, according to Kaminski, should impose an obligation to inform individuals about new surveillance methods so they can adjust accordingly. Furthermore, legal regulation should not only protect privacy but also prevent undesirable changes in human behavior.

The boundary management theory suggests that laws should be based on preserving desirable behavioral norms rather than focusing on specific technological features or types of collected information. This approach would help avoid overly restrictive technological regulations and encourage public discussion on socially significant behavioral standards. In this way, legislators – rather than courts – would determine which behavioral changes are acceptable and which should be regulated.

3.2.4. Subsection Conclusions: Theoretical Basis for Future Regulation of Privacy in Public Spaces in the Context of Drones

The analysis of privacy regulation models in public spaces highlights three main approaches: H. Nissenbaum's theory of contextual integrity, J. Reidenberg's public significance model, and M. E. Kaminski's boundary management theory. H. Nissenbaum's theory focuses primarily on the use of already collected information but does not sufficiently address the act of data collection itself. Since drones are primarily tools for data collection, this theory does not provide adequate privacy protection.

J. Reidenberg's public significance model shifts the burden of resolving disputes onto courts, requiring them to determine whether specific data is of public interest. In practice, this approach is not significantly different from the binary privacy theory, which has been deemed ineffective in the context of drones.

M. E. Kaminski's boundary management theory proposes regulating privacy based on behavioral norms that society seeks to preserve or limit. This approach would reduce the burden on courts and encourage public engagement while ensuring that technological advancements are not unnecessarily restricted. Therefore, this theory is suggested as the most suitable foundation for shaping new legislation and judicial practices in Lithuania and the EU.

3.3. The Relationship Between Drone Use in Public Spaces and Privacy in ECtHR and Lithuanian Jurisprudence

3.3.1. The Relationship Between Privacy and Public Spaces in ECtHR Jurisprudence

The right to private life in EU law is enshrined in Article 8 of the European Convention on Human Rights (ECHR), which protects privacy from arbitrary state interference and obliges states to respect privacy even in interactions between private individuals. The ECtHR's jurisprudence on privacy in public spaces is based on the "reasonable expectation of privacy" standard – while individuals may expect privacy, any infringement is assessed based on factors such as systematic surveillance, the nature of monitoring, and the use of collected data.

Court rulings have established that workplaces and university auditoriums may have some degree of privacy protection if specific relationships develop within them. Covert employee surveillance may be considered a privacy violation if the principle of proportionality is not observed, but in certain cases, it has been deemed lawful when necessary and proportionate to achieving an employer's objective.

The *Big Brother Watch* case demonstrated that the ECtHR recognizes the legitimacy of mass surveillance if it meets clear legal conditions. However, this position has been criticized for allegedly granting states excessive discretion and failing to ensure real privacy protections.

General trends indicate that judicial practice is increasingly tolerant of state surveillance, raising concerns about the actual guarantees of privacy protection.

3.3.2. The Relationship Between Privacy and Public Spaces in Lithuanian Jurisprudence

In Lithuanian law, privacy limitations in public spaces are regulated through the right to one's image (Article 2.22 of the Civil Code) and the right to private life (Article 2.23 of the Civil Code). A person's image may be recorded without consent in public spaces, but unauthorized surveillance, including audio recording, is not explicitly defined. The Law on Public Information does not establish a clear prohibition on data collection in public places, and Lithuanian courts often address the right to an image and the right to private life together.

The jurisprudence of the Lithuanian Supreme Court (LAT) indicates that privacy is not entirely lost in public spaces. Courts consider not only the nature of the space but also additional criteria, such as an individual's objection to being recorded. The concept of a public space is not strictly defined but generally includes streets, shops, parks, and other shared-use areas. Private spaces are understood as residential environments, private property, and certain workplaces.

LAT rulings show that even in public spaces, filming an individual may be prohibited if they clearly express their objection. In cases involving image or data publication, courts assess not only the act of recording but also the context of dissemination. However, legal disputes regarding data collection without public disclosure are virtually nonexistent.

State institutions may limit privacy based on public security concerns, but Lithuanian intelligence agencies have broad discretion to conduct surveillance, which has been criticized for vague legal boundaries and the potential for abuse. Mass surveillance regulation in Lithuania is generally considered to favor state interests over privacy, and some experts argue that Lithuanian practices may not meet even the minimum standards set by the ECtHR.

3.3.3. Assessment of ECtHR and Lithuanian Jurisprudence on Privacy in Public Spaces in the Context of Drones

A comprehensive analysis of ECtHR and Lithuanian jurisprudence on privacy in public spaces allows for an evaluation of how these legal precedents may influence privacy issues arising from drone use. Lithuanian jurisprudence on this matter is underdeveloped and does not specifically address drones, making it necessary to rely on ECtHR case law when assessing these issues.

The ECtHR takes a differentiated approach to privacy boundaries in public spaces, depending on whether surveillance is conducted by state authorities or private entities. Stricter regulatory criteria apply between private entities, whereas states are granted broader discretion to establish surveillance measures, provided they comply with legal requirements. According to ECtHR practice, drone operators conducting surveillance in public spaces should inform individuals about data collection, though implementing this obligation may be challenging. If surveillance does not involve data recording, there may be no duty to inform; however, this conclusion is based on cases concerning stationary CCTV surveillance, whereas drones, due to their mobility, may pose a greater threat.

The ECtHR also emphasizes the scope of surveillance and the degree of intrusion into private life. Targeted or continuous monitoring of an individual, even in public spaces, may be considered excessive interference with privacy. Certain public areas, such as nudist beaches or locations where individuals deliberately isolate themselves using physical barriers, may be regarded as more private, making their surveillance a potential privacy violation.

Additionally, the ECtHR requires that surveillance have a clear legal basis, with more intensive surveillance requiring stronger justification. Legislators should clearly define which segments of public spaces allow surveillance and where it is restricted or prohibited. Such legislative clarity would help individuals better understand where their actions may be monitored and recorded.

State surveillance is subject to more lenient requirements under ECtHR case law. In *Big Brother Watch,* the court ruled that mass surveillance by states is permissible if it adheres to specific procedural safeguards. However, this practice has been criticized for potentially weakening privacy protections. In Lithuania, intelligence agencies are granted broad surveillance powers, despite concerns about insufficient judicial oversight.

4. DRONES AND DATA PROTECTION

Data protection is a crucial aspect of the right to privacy, especially in an era where advanced technologies allow for large-scale data collection, automatic transmission, and aggregation. As previously mentioned, drones pose a significant threat to data protection due to their ability to collect vast amounts of information. They can also contribute to data processing violations such as aggregation, identification, and security breaches. In the EU, data protection is governed by the GDPR, which will be analyzed in this dissertation in relation to drone usage. This chapter addresses the fifth and sixth research objectives.

The first subsection examines how the GDPR applies to drones. The second defines the legal grounds for data collection. The third analyzes the privacy protection measures proposed by the GDPR and assesses whether they provide sufficient safeguards against the risks associated with the increasing use of drones. The fifth subsection discusses the shortcomings of the current consent-based privacy protection system. The sixth presents the author's recommendations for future privacy regulation.

It is important to note that the sixth subsection does not aim to provide a detailed structure or wording for potential legal acts. The dissertation's objective is to analyze the current privacy regulation of drone usage and specialized drone regulations, offering suggestions for their improvement. Given the continuous technological advancements and the evolving legal landscape, overly specific legislative modeling could limit the flexibility of these proposals and hinder their applicability across different contexts.

For this reason, the dissertation emphasizes the development of regulatory principles and application directions rather than the formulation of specific legal provisions. This approach maintains a balance between privacy protection and the technological development of drones, allowing legislative bodies and market participants to adapt the proposed guidelines to changing circumstances. Such a method also ensures that the proposed solutions remain flexible enough to facilitate innovation while enhancing legal clarity and preventing potential misuse.

4.1. How the GDPR Applies to Drone Use

The GDPR applies to drone operations when they involve the processing of personal data, including data collection, recording, structuring, and other related activities. However, the regulation is only applicable if the collected information enables the identification of an individual. Pseudonymized data falls within the scope of the GDPR, whereas anonymized data does not.

The GDPR does not apply when data is collected exclusively for personal or household purposes. However, CJEU case law indicates that this exception does not extend to data collection in public spaces, even if conducted by a private individual. Nevertheless, applying this interpretation to drones may be impractical and disproportionate, as private individuals typically do not engage in systematic personal data collection. The final interpretation of the GDPR's applicability to drones may be shaped by future rulings of the CJEU or guidance from data protection authorities.

Additionally, the GDPR does not apply when data is processed by public authorities to ensure public security or prevent criminal activities. Since the GDPR does not contain specific provisions on drones, the regulation's scope is left to national legislators, courts, and market participants. This dissertation's analysis will focus on the legal grounds for drone data collection and the privacy protection measures proposed by the GDPR.

4.2. The Bases for Data Collection with Drones

The next step is to examine the legal grounds under which data collection by drones would be lawful under the GDPR. Article 6 of the GDPR specifies the following lawful bases for data processing:

a) the data subject has given consent;

b) data collection is necessary for the performance of a contract;

c) data collection is required to comply with a legal obligation applicable to the data controller;

d) data collection is necessary to protect the vital interests of the data subject or another individual;

e) data collection is necessary for the public interest;

f) data collection is necessary based on legitimate interest.

The author of this dissertation argues that a detailed discussion of grounds (b), (c), (d), and (e) is unnecessary, as they do not raise significant issues in the context of drones. However, grounds (a) and (f) require further analysis.

One proposed approach is to regulate drone usage based on the boundary

management theory, where private entities would process data under the framework of a national legal act. The GDPR does not explicitly provide such a legal basis in Article 6, making it necessary to examine whether implementing this proposal would be lawful under the GDPR.

4.2.1. Consent as a Basis for Data Collection by Drones

The GDPR requires that consent for data collection be freely given, specific, informed, unambiguous, and easily revocable. However, in practice, obtaining prior consent from all individuals present in a public space is often impossible. Private individuals flying drones recreationally typically lack the means to meet GDPR consent requirements. As a result, they would need to adopt alternative measures, such as operating drones in unpopulated areas, anonymizing data, or avoiding recording altogether.

For commercial operators, obtaining consent may be more feasible, but in large public gatherings or open spaces, it remains challenging. In such cases, other GDPR legal bases may apply, such as legitimate interest or a national legal provision, as well as technological solutions that enable data anonymization before storage.

In conclusion, while consent is a possible legal basis for data processing, its practical application in the context of drones is limited. Therefore, alternative legal frameworks or technological solutions must be explored.

4.2.2. Legitimate Interest as a Basis for Collecting Data with Drones

The "legitimate interest" provision outlined in Article 6(1)(f) of the GDPR can serve as a basis for collecting data using drones, but its abstract formulation poses a risk of misuse by major data controllers. This basis allows for data collection without the consent of the subject, but it is necessary to demonstrate that the interest is legitimate, the processing of data is essential, and it does not violate the rights of individuals.

The Court of Justice of the European Union (CJEU) emphasized that legitimate interests must align with the rights of data subjects. The European Data Protection Board (EDPB) indicates that this basis can be applied for purposes such as journalism, scientific research, or uncovering illegal activities; however, it does not permit data marketing in this manner without consent.

The author of the dissertation assesses that legitimate interest could be an appropriate basis for the use of drones under certain circumstances, but the principles of proportionality and necessity must be observed to avoid excessive surveillance and breaches of individual privacy.

4.2.3. National Legislation as a Basis for Collecting Data with Drones

The dissertation proposes regulating the use of drones based on the "boundary management" theory, which would eliminate the need for drone operators to obtain consent from individuals being observed. In such cases, the basis for data processing would not rely on individual consent but instead on national legislation that establishes clear limits applicable in public spaces. While the GDPR does not directly specify such a basis, it grants Member States some discretion to further regulate the grounds for data processing under Article 6(2).

According to this provision, states may adopt new laws or clarify existing ones, provided they align with the data processing grounds outlined in the GDPR. Article 6(3) of the GDPR highlights the requirements such regulation must meet: clearly defined purposes for data processing, storage duration, subjects of the data, and their rights. Furthermore, any national regulation must be proportionate and not contradict public interest objectives.

Although the GDPR and EDPB guidelines do not provide a definitive answer as to whether such regulation would be lawful, a systematic evaluation of the provisions suggests that it could fit within both points (c) and (e) of Article 6(2). This would mean that national legislation based on a boundary management mechanism could serve as a viable alternative to individual consent, without conflicting with GDPR requirements.

4.2.4. Subchapter Conclusions

The processing of data collected via drones is primarily based on either the consent of the data subject (Article 6(1)(a) of the GDPR) or legitimate interest (Article 6(1)(f) of the GDPR). While consent is theoretically suitable, it is difficult to implement in practice, especially in public spaces where obtaining prior consent from all individuals is often impossible. Such a requirement would impose overly restrictive limitations on both private and commercial users.

The legitimate interest basis can be applied in cases of journalism, scientific research, or public interest, but its abstract nature can lead to differing interpretations. Therefore, it is essential to ensure the principle of proportionality so that the rights of data subjects are not infringed beyond what is necessary.

An alternative solution could be national regulation under Article 6(2) of the GDPR. This would allow for clearer definitions of the boundaries for drone use, achieving a balance between privacy protection and technological progress. It would also enable data collection without consent in certain cases, provided there is no systematic surveillance or easy identification of individuals.

4.3. Privacy Protection Measures Proposed by the GDPR

When transitioning to the privacy protection measures proposed by the GDPR related to drones, it is important to discuss the key general requirements for personal data processing under the GDPR, the principles of data protection by design and by default, data pseudonymization, and data protection impact assessments.

4.3.1. General Requirements for Personal Data Processing

The GDPR does not specify separate requirements for drone surveillance; therefore, their data processing must comply with the general principles enshrined in Article 5 of the GDPR: legality, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, protection of subjects' rights, and accountability. These principles include the obligation to inform observed individuals, collect only necessary data, ensure its accuracy, store it for a limited time, protect it from unauthorized access, and allow individuals to access the data collected about them.

Although GDPR principles are abstract and do not provide specific guidance for drone operators, their flexibility enables market participants to establish good practices. As technology and its usage evolve, jurisprudence is expected to refine practical standards. Over time, this may lead to more tailored legal regulation that, based on boundary management theory, could promote technological development while ensuring privacy protection.

4.3.2. Privacy by Design and by Default

Articles 25 and Recital 78 of the GDPR introduce the principles of privacy by design and privacy by default, encouraging the integration of privacy protection into all market processes for drones – from design to operation. National authorities and market participants have the discretion to choose measures, but these must align with the level of technological development, the nature, scope, and context of data processing, and potential risks to individuals' rights.

The Lithuanian State Data Protection Inspectorate (VDAI) provides recommendations for video data processing, which, although not directly related to drones, illustrate potential data protection requirements. For instance, video recordings should not be stored longer than necessary, access to data should be restricted to authorized personnel, and unique access control measures should be implemented to ensure security.

Since GDPR principles are quite abstract, they do not always offer clear guidance to drone operators. However, this regulatory flexibility allows market participants to adapt to technological developments and encourage self-regulation, which might eventually form the basis for specific legal regulation in this field.

4.3.3. Pseudonymization, Encryption, and Anonymization of Data

The GDPR specifies pseudonymization, encryption, and anonymization as measures that can ensure greater protection of personal data. Pseudonymization refers to the encryption of data so that it cannot be attributed to a specific person without additional information, although it still remains personal data. Encryption makes data unintelligible without a decryption key, reducing the number of entities that can access it. Anonymization, on the other hand, irreversibly removes the ability to identify individuals, which means such data falls outside the GDPR's scope.

In the context of drones, encryption and pseudonymization can already effectively protect data by limiting access and reducing the risk of misuse. Theoretically, anonymization would be an even more effective privacy protection measure, but current technology is not yet advanced enough to ensure reliable real-time depersonalization. Moreover, there is a risk that anonymized information could be de-anonymized, particularly when data controllers aim to analyze societal behavior patterns.

Until anonymization technologies reach a higher level of security, the primary privacy protection measures for drones should consist of encryption and pseudonymization. In the future, if anonymization becomes more widely applied, it is essential to ensure that laws limit the retention period of such data to prevent misuse.

4.3.4. Data Protection Impact Assessments

The GDPR mandates Data Protection Impact Assessments (DPIA) as a preventive measure to identify and mitigate risks to human rights, including privacy, when using innovative technologies such as drones. DPIA is required in cases of systematic public surveillance, profiling, processing special categories of data or large-scale data, or the use of new technologies.

Guidelines from the Lithuanian State Data Protection Inspectorate (VDAI) outline four key stages of DPIA:

1. Defining the context of data processing: Identifying what data is processed, for what purposes, and the methods used.

2. Risk assessment: Evaluating the likelihood of threats and potential consequences, ranging from minor inconveniences to severe legal, financial, or health issues.

3. Identifying threats: Analyzing data security gaps and potential breaches.

4. Implementing preventive measures: Introducing both organizational (e.g., internal data protection policies, training, security procedures) and technical (e.g., encryption, two-factor authentication, access control) measures.

DPIA helps organizations preemptively evaluate privacy risks, reduce the likelihood of unexpected data breaches, and encourage self-regulation in the tech market. It can be seen as one of the tools of the boundary management theory, aiding in maintaining a balance between innovation and privacy protection.

4.4. Assessment of the GDPR in the Context of Drones and Privacy

Drones fall under the scope of the GDPR as they can be used to collect personal data, though GDPR requirements do not always apply. If individuals cannot be identified or the data is anonymized, strict GDPR rules are not mandatory.

The most likely GDPR bases for drone data processing are the consent of the data subject and legitimate interest. However, obtaining consent in public spaces is challenging, so medium-scale users or entities conducting large-scale surveillance may require alternative legal bases. Case law from the Court of Justice of the European Union (CJEU) indicates that GDPR should formally apply even to recreational drone usage by private individuals, but such interpretation might be disproportionate.

Legitimate interest could serve as an appropriate basis in certain cases (e.g., journalism or scientific research), but the abstract nature of GDPR provisions raises the risk of misuse. Nevertheless, analysis suggests that courts would likely interpret this provision narrowly to prevent excessive power concentration among large data controllers.

Among the GDPR's proposed privacy protection measures, encryption and Data Protection Impact Assessments (DPIAs) are considered the most effective. Additionally, general personal data processing rules and privacy by design and by default principles promote self-regulation and encourage privacy standardization in the drone market.

Although anonymized data falls outside the GDPR's scope, there have been instances of de-anonymization. Therefore, the dissertation's author recommends setting retention periods for anonymized data to prevent privacy violations.

Overall, GDPR is an abstract yet flexible regulation that allows national authorities and market participants to shape privacy protection standards themselves. However, the consent requirement for drones in practice proves highly impractical, highlighting the need to explore other effective privacy protection mechanisms.

4.5. Drawbacks of Consent-Based Privacy Protection Systems

EU data protection law and specific drone regulations are based on the paradigm of self-managed privacy, where privacy protection depends on user consent. However, research shows significant shortcomings in this system. The "privacy paradox" highlights that while users claim to value privacy, their behavior often contradicts this, as they frequently agree to data processing without much consideration.

The six main reasons why consent-based privacy protection is ineffective are:

1. Unclear consequences of data processing: Privacy policies are often complex, and shorter information fails to reveal the full implications of data use.
2. Limited rationality of individuals: Users struggle to properly assess risks and rely on simplified decision-making strategies.
3. Forced consent: Users often have no real choice, as online services and technologies require data processing.
4. Excessive number of consents: People encounter numerous data processing requests daily, leaving them no time for thorough analysis.
5. Unpredictable consequences of data use: Personal data can later be aggregated and interpreted, even if it was initially collected anonymously.
6. Short-term benefit priority: Users exchange their personal data for small, immediate benefits, failing to consider long-term consequences.

Due to the power and knowledge asymmetry between users and data controllers, consent-based privacy protection is often ineffective. Large companies can manipulate consents by using psychological strategies that encourage users to unknowingly share more data.

Paternalistic regulation is an alternative to self-managed privacy. In this approach, the state sets privacy protection standards without requiring individual consent. Examples include seatbelt requirements or drone registration rules. The GDPR also contains paternalistic elements, such as requirements for data processing without consent and principles of privacy by design and by default.

Despite the GDPR's efforts to address the shortcomings of self-managed privacy, the question of whether the current regulation sufficiently protects users remains open. In the context of drones, consent-based privacy regulation appears ineffective, highlighting the need for alternative protective measures.

4.6. Guidelines for Improving Regulation Through Boundary Management

The analysis revealed that both the GDPR and specific drone regulations rely on the consent of the observed individual. However, in practice, this does not ensure independent decision-making by individuals due to various reasons, including the inherent limited rationality of people. The GDPR attempts to address these issues with paternalistic provisions that impose strict requirements on data controllers for data processing. Preventive privacy protection measures outlined in specific drone regulations could complement these efforts. To assess whether such requirements balance the shortcomings of self-managed privacy, each data processing operation should be examined individually. In the context of drones, such a study would be relevant if obtaining consent from data subjects were as easy as browsing the internet. However, as earlier sections of the dissertation demonstrated, obtaining consent for data collection via drones is particularly challenging. Therefore, evaluating the balance between self-managed privacy and paternalistic measures in the context of drones is unnecessary.

The problem with the consent requirement for drones is much simpler – it is simply difficult to obtain. In the real world (unlike online), there is currently no mechanism that could automatically inform all individuals in the area of a drone flight about the planned flight and stop collecting their data upon their objection. An analysis of sources regulating drones, covered in an earlier dissertation chapter, shows that the International Civil Aviation Organization (ICAO) addresses the issue by proposing minimal consent requirements, such as implied consent. However, even the mere inclusion of this consent form in regulations opens the door to potential misuse by drone operators. In the United States, there is a view that there is no formal need to mandate informing and obtaining consent from nearby individuals, leaving this responsibility as a recommendation only in cases where drone operators believe they may intrude into personal space. Meanwhile, EU requirements for consent are strict and comprehensive but practically unfeasible for flights in crowded areas. According to the dissertation author, none of these approaches achieves a balance between adequate privacy protection and technological advancement in drones. EU consent requirements are too strict, stifling innovation, while the approaches of the US and ICAO are too lenient, failing to ensure sufficient privacy protection.

To strike a balance between the right to privacy and technological advancement in drone use, the boundary management theory discussed in earlier chapters of the dissertation is suitable. This theory focuses on behavior patterns that norms aim to preserve (or, conversely, suppress for greater good). The appeal of this regulatory model lies in its simplicity and its ability to spark societal discussions about how privacy in public spaces should be regulated. Greater public involvement in decision-making and the visibility of boundary management protections should promote individual and group autonomy, preventing a "chilling effect." Applying this theory could simplify legal disputes over privacy in public spaces and ensure that technological progress is not unreasonably hindered over time. This theory is inherently paternalistic, proposing to establish behavior patterns to preserve (or suppress) through mandatory legal acts enacted by the legislature (or local government bodies), often leaving individuals no choice to agree or disagree with the established standard.

To further discuss regulatory measures for practical implementation of this proposal, the concept of regulation defined in an earlier chapter of the dissertation is followed. It is understood to consist of six primary regulatory methods: information-based regulation, self-regulation, co-regulation, standardization, market measures, and formal regulation. The methods required for implementing the regulatory model proposed by the dissertation author are formal regulation, information-based regulation, and standardization. It is worth discussing in detail how each of these could be applied in boundary management and analyzing why other methods are unsuitable.

Initially, the functioning of drone regulation through boundary management theory would be based primarily on formal regulation. This method ensures that there are no questions in judicial practice or society about what is considered an acceptable standard of behavior in privacy-related situations. According to the dissertation author, in most cases, sufficient authority to implement decisions related to drone flights and information gathering in public spaces should rest with the government or municipalities. However, in the future, as the issue of privacy protection in public spaces due to drone usage intensifies, these relationships could be regulated at a higher level. Legislatures (parliaments) could enact mandatory legal acts (laws) that define and establish the boundary management mechanism nationwide. The law could stipulate that behavior patterns to preserve (or suppress) are determined by the executive branch (government) through separate resolutions or local authorities.

Examples of when the relationship between drone operators and society might need clearer regulation can be imagined through specific cases. For illustrative purposes, two potential future scenarios are provided below.

Situation 1	
A retail association in Lithuania seeks to use drones equipped with artificial intelligence and machine learning algorithms to improve store layouts and advertising effectiveness. These drones would fly over major city shopping areas, collecting data on customer movement patterns, time spent near various stores, and interactions with advertisements. The collected data would be analyzed by AI models to generate recommendations for optimal store placement, advertising locations, and content.	
Problem	The retail association is unable to implement this idea because, under the GDPR, conducting such surveillance in public spaces would require obtaining consent from all observed individuals.
Solution	Local government authorities could establish a permit system for conducting public space surveillance. Under this system, entities planning to carry out drone-based surveillance could apply for permits from the local authorities. The application process could require submitting a completed Data Protection Impact Assessment (DPIA), enabling the applicant to justify in advance why their surveillance would not excessively infringe on individuals' privacy or why any intrusion into personal privacy would be reasonable. The local authorities could outline criteria for issuing permits based on the boundary management theory. A permit issued to the retail association could then serve as a legal basis for data collection under Article 6(2) of the GDPR (national legislation as a basis for collecting data with drones). This would align technological innovation with privacy protection by formalizing and standardizing the process.

Situation 2	
Municipalities in large cities, in collaboration with technology companies, plan to implement Smart City technologies aimed at improving the quality of life for city residents, enhancing safety, and fostering economic growth. One of the key initiatives involves using drones to collect data on city infrastructure usage, population movement, and behavioral patterns. Small, inconspicuous drones equipped with advanced sensors and artificial intelligence algorithms would fly over urban areas to gather data on traffic flows and road conditions, pedestrian and cyclist routes, public transport usage and stop frequency, public space and park attendance, air quality and pollution levels across different city zones, and the energy efficiency and consumption of buildings. The collected data would then be processed by AI systems capable of real-time analysis. These systems would provide insights and recommendations to help municipal authorities and business entities develop new products and services.	
Problem	Municipalities cannot implement this initiative as, under the GDPR, such surveillance in public spaces requires the consent of all observed individuals. Furthermore, continuous population surveillance by drones poses a clear threat to citizens' privacy. Municipalities implementing such a solution through secondary legislation risk legal disputes over violations of the right to privacy.

Solution	In this case, a national law could serve as the basis for data collection under Article 6(2) of the GDPR, eliminating the need to obtain consent from all observed individuals. The state could enact a national law based on the boundary management theory, defining which behavioral patterns are to be preserved (or suppressed). Municipalities could use secondary legislation to specify the measures for preserving or reasonably limiting such patterns. The law could stipulate that the following behavioral patterns are to be preserved: - **Personal time in public parks:** The law could state that spending leisure time in public parks is important because people communicate with each other on private topics there and want to relax knowing they are not constantly monitored. Municipalities, through secondary legislation, could define how specifically this behavioral pattern will be preserved. For example, drone flights in public park areas could be conducted at an altitude no lower than 150 meters. Alternatively, drone flights over parks could be completely prohibited, or Smart City infrastructure drones could be banned from flying over parks entirely. - **Participation in public cultural and religious events:** The law could state that, for example, at concerts, performances, or religious services, people must be protected from constant monitoring since in such events individuals also have a legitimate expectation to be monitored only when necessary for safety. Municipalities could, through secondary legislation, define specific surveillance requirements, such as prohibiting Smart City drone flights during cultural and religious events. - **Conversations in public spaces:** The law could stipulate that, for example, active surveillance by drones should not be conducted on cafe terraces or public squares. Municipalities could restrict or completely prohibit drone use in such places. The law could also define cases where preserved behavioral patterns could be suppressed with higher levels of intrusion through drone surveillance for the greater good, for example: - **Monitoring vehicle traffic for safety purposes:** To ensure traffic safety, monitoring vehicle speed with drones could be allowed. Municipalities could establish specific rules for how drones could record vehicle speeds and transmit this data to law enforcement to reduce speeding incidents and improve traffic conditions in cities. - **Monitoring public spaces and events for security purposes:** Monitoring some or all public spaces to ensure public safety could be allowed. Municipalities could further detail regulations in their laws, such as the type of drones allowed in certain areas or events. Alternatively, drone surveillance could be conducted through periodic flyovers, or drones in certain areas could use only specific types of sensors. - **Ensuring health protection:** To improve the accessibility and efficiency of healthcare services, the law might permit the use of highly privacy-intrusive drones that can detect signs of health issues, such as heart attack symptoms, fainting cases, or other critical health conditions. Municipalities, through secondary legislation, could again impose certain technological restrictions on data collection or introduce advanced solutions enabling better data collection, depending on the law's provisions.

As mentioned in the previous chapter of the dissertation, the application of boundary management theory would encourage society to engage in legal discussions about significant behavioral patterns that it wishes to protect. This should promote individual and group autonomy within society and help avoid the chilling effect. The opportunity for public participation in discussions is ensured by any legislative process in democratic systems. The formal regulatory process begins with legal ideas, which are transformed into legal norms during the legislative process. In Lithuania, for a concept to become a legal act, a draft law must be initiated in the

Seimas by one of the entities specified in Article 68 of the Constitution of the Republic of Lithuania. A newly registered draft is further sent to the relevant Seimas committees and commissions, which review and prepare it for coordination, inter alia, with public organizations, social groups, as well as to be published in the media and online for the public to familiarize themselves with. It is at this stage of drafting the legal act that the public should have the opportunity to participate in legal discussions about behavioral patterns to be protected or suppressed.

It is noteworthy that, in Lithuania, orders prepared by ministries are not pre-coordinated with the public in the same manner as draft laws. Therefore, the dissertation author recommends implementing drone regulation through the boundary management theory via the legislative branch. The executive branch should adopt orders concerning boundary management mechanisms in public spaces only in exceptional cases requiring a quick decision. To involve the public in discussions, any regulations governing the relationship between drone operators and society established by the Government should later be incorporated into laws.
Information-based regulation in the context of the theory proposed by the dissertation author would be applied indirectly. For individuals to adjust their behavior according to the amended privacy boundaries in public spaces, formal regulation based on boundary management theory should establish an obligation to inform. This requirement should be implemented by public authorities, which would announce new laws implementing boundary management mechanisms through the media. Additionally, informational signs could notify passersby about newly enforced boundary management mechanisms in specific areas.

Standardization, as a regulatory method, implies that an institution with the authority of formal regulation grants a mandate to a governmental organization to create advisory standards. The organization involves interested individuals and legal entities in the standard-setting process. For example, in Lithuania, the State Data Protection Inspectorate (VDAI) performs standardization in the area of data protection. According to the dissertation author, this regulatory method should be applied in the case of drones to make formal regulation more comprehensible to the public and businesses.

Guidelines and recommendations could provide practical scenarios for the application of formal regulation. Furthermore, market players could contribute their experiences to these guidelines, incorporating public input into the decision-making process.

As technologies continuously evolve, the importance of self-regulation increases because formal legal regulation lags significantly behind technological progress. Various reasons may explain delays in formal regulation: authorities may lack the expertise to regulate new phenomena, or they may delay to avoid

unjustifiably hindering technological progress. It might also be deemed too costly to regulate such relationships, or the state authorities may consider that leaving the relationships unregulated poses no significant risk to society. Self-regulation is often implemented by non-governmental organizations uniting market players, which approve guidelines regulating relationships or standards and provide training. In Lithuania's drone market, this could include the Lithuanian Drone Users Association, established in 2014. In the field of data protection, the Privacy Protection and Data Protection Association (APGIDA), established in 2019, operates in Lithuania. Non-governmental organizations, contributing to the proposed drone regulation through boundary management theory, could only participate in the formal regulation process by submitting proposals from their association members. However, self-regulation solutions within the context of boundary management theory would not be effective because private companies, even if they establish boundary management mechanisms in public spaces, would not have a legal basis for processing data without data subject consent, which, as already discussed, is difficult to obtain in the context of drones.

The essence of co-regulation is to establish abstract objectives through legislation for recognized non-governmental entities (economic entities, social partners, non-governmental organizations, or associations), allowing them to set their standards based on these objectives. This regulatory method, when applying the boundary management theory, would also not be acceptable due to its abstractness. Behavioral patterns to be preserved (or abandoned) and boundary management mechanisms must be very clearly defined. Otherwise, there would be extensive debates in society and judicial practice about the applicable boundary management mechanism, and data controllers would question whether they violate GDPR requirements in specific cases.

Finally, market-based measures are instruments through which the state provides positive or negative monetary incentives to market players, setting the basic rules of the game (compensations, permit sales, taxes, fees, property and liability rules, licenses, quotas, etc.). According to the dissertation author, these measures are more suitable for legal areas such as environmental protection. It is challenging to imagine how they could be applied to the field of privacy protection; therefore, this regulatory measure would not be appropriate for protecting privacy from the threats posed by drones.

The analysis revealed that self-managed privacy based on individual consent has its flaws. When providing consent for data processing, individuals often do not understand the actual implications of their choice or perceive them somewhat distortedly due to inherent limited rationality. Additionally, it can be argued that individuals do not have real autonomy to make decisions under current

market conditions because economic models that collect less data simply do not exist. People lack the time to read privacy policies and cannot accurately foresee the long-term consequences of data processing and aggregation. One solution suggested in the academic literature is paternalistic regulation, which essentially restricts individual freedom of choice for their benefit. Paternalistic provisions are abundant in various modern legal acts, including the GDPR and specific drone regulations.

The drone regulation model proposed by the dissertation author is also paternalistic. It is based not on consent but on mandatory behavioral rules grounded in formal regulation. This regulatory model is appealing because it is straightforward. Its application could simplify judicial processes, and discussions about how privacy should be regulated in public spaces could actively involve society. According to the dissertation author, the proposed regulation could be implemented through formal regulation, information-based regulation, and standardization.

Conclusions. Summarizing the research conducted, the dissertation author concludes that the research aim specified in the introduction has been achieved, the objectives have been fulfilled, and the defended statements have been validated. This is substantiated by the following findings:

1. The research conducted in the dissertation revealed that drones pose a threat to privacy through violations such as surveillance, aggregation, identification, lack of security, and exposure. These violations arise because drone technology possesses unique characteristics not found in any other surveillance tool currently available. These characteristics include a large scale of use, high intensity of surveillance, a variety of observation angles, the potential to become a weapon, and stealth. As the research has shown, the distinctive capabilities of drones enable both states and powerful market entities to create infrastructure for opportunistic information gathering in the real world. Consequently, without proper regulation of drone use, a chilling effect may occur, leading to undesirable psychological changes among individuals, behavioral shifts within social groups and different societal layers in a negative direction, and threats to the stability of the democratic order.

2. Among the specialized drone regulations examined, adopted by ICAO, JARUS, the EU, and the US, it is evident that only EU drone regulations explicitly establish privacy protection. However, this does not mean that other analyzed sources do not include privacy protection measures – such measures are embedded indirectly. The analysis showed that current specialized drone laws contain several preventive measures that could help mitigate privacy violations: (a) distance compliance requirements; (b) the requirement to inform or obtain consent; (c) registration requirements; (d) requirements to store recordings; (e) qualification requirements for drone pilots; (f) risk assessment requirements; (g) remote identification

attachments; (h) geographic orientation attachments (geo-restriction); (i) ensuring security in data transmission communication lines; (j) the requirement to manufacture drones with lights. According to the dissertation author, while all these measures could theoretically reduce the likelihood of privacy violations to some extent, many of them currently fail to provide real prevention due to deficiencies in regulatory provisions and the underdevelopment of privacy-protecting technologies.

3. An analysis of scientific literature on privacy in public spaces identified three dominant theories in academic discourse, on which foreign authors base their proposals for regulating privacy boundaries in public spaces: (i) the theory of contextual integrity, (ii) the theory of societal significance, and (iii) the boundary management theory. Each of these theories was analyzed to determine whether any of them could create a balance between privacy in public spaces and technological progress. The research showed that the theory of contextual integrity would not provide sufficient privacy protection against violations caused by small drone usage. This theory primarily examines the legality of the further transfer and comparison of already collected information, but it does not focus on the legality of data collection itself, which is crucial in the context of drones. According to the dissertation author, the theory of societal significance would also fail to provide adequate privacy protection. Applying this theory, courts would have to determine which right is superior – the right to privacy or the right to freedom of expression – placing an excessive burden on judicial systems. This regulatory model offers almost no added value compared to the outdated binary theory, which prioritizes whether information was collected in a public or private space, essentially using a territorial distinction between public and private domains. Finally, the boundary management theory, according to the dissertation author, could simplify the legislative process, ease legal disputes related to drone usage, and avoid overly restricting drone technological advancements. Applying this model should also encourage public participation in decision-making during legal regulation processes, fostering both individual and collective self-governance and autonomy, thus helping to prevent the chilling effect.

4. The analysis of ECtHR and Supreme Court of Lithuania (LAT) case law related to privacy boundaries in public spaces revealed that courts have not yet addressed cases involving drone usage. In Lithuanian Supreme Court jurisprudence, privacy-related cases are relatively few, and they lack universally applicable legal rules. Consequently, drawing conclusions about future Lithuanian court reasoning in drone-related cases would be premature. From the ECtHR case law, which Lithuanian courts are required to follow, it is evident that the assessment of privacy boundaries in public spaces varies significantly depending on whether surveillance

is conducted by a private individual or a government entity. Established legal practice suggests that private entities conducting drone surveillance should be more strictly supervised and regulated, yet existing case law remains too abstract for judges to rely on in cases concerning the relationship between drone usage and privacy without an additional theoretical foundation. The boundary management theory, as proposed in the dissertation, provides such a theoretical foundation and aligns with the universal legal principles already established by the ECtHR. The public space surveillance by government entities using drones, according to established ECtHR case law, would face almost no restrictions due to a recent ruling favoring mass surveillance in the case "Big Brother Watch and Others v. the United Kingdom". This ruling grants states broad discretion in determining the extent to which individual privacy can be restricted in the interest of national security. According to the dissertation author, secret mass surveillance, regardless of whether it is conducted by government authorities or private individuals, would always violate privacy rights from a substantive legal perspective. This is because individuals under surveillance, being unaware of it, cannot adjust their behavior accordingly. It is believed that currently, the only factor that could prevent the implementation of secret drone surveillance is strong international or national political will to reject mass state surveillance. As the research has shown, Lithuanian legislation, although criticized by Lithuanian courts, is being amended in a direction unfavorable to privacy protection.

5. As the analysis of EU data legislation has shown, unmanned aerial vehicles fall within the scope of the GDPR, as they are tools for data collection. The GDPR would not apply to data collection by unmanned aerial vehicles only in cases where the collected material does not allow the identification of individuals or when the data is presented in an anonymous form. Among the lawful bases for data processing that unmanned aerial vehicle operators could rely on, the author of the dissertation considers the most likely to be the data subject's consent (Article 6(1)(a) of the GDPR) and "legitimate interest" (Article 6(1)(f) of the GDPR). The dissertation author has identified another realistic basis for data collection by unmanned aerial vehicles that is not explicitly provided for in the GDPR – national legislation. The analysis showed that, according to the CJEU's case law developed in the context of stationary CCTV cameras, even ordinary users conducting flights in public spaces should obtain the consent of those around them. However, in the author's assessment, the GDPR provisions should probably not apply to average users conducting flights for personal purposes, and therefore, it would not be appropriate to follow this CJEU case law. In evaluating the privacy protection measures proposed by the GDPR, it was concluded that encryption solutions and data protection impact assessments provide the greatest benefits. Anonymization was specifically

discussed as one of the encryption solutions, as data processed in this way would fall outside the scope of the GDPR. However, the current anonymization technology is not sufficiently developed and therefore cannot be widely applied. Furthermore, it is criticized that current legislation does not specify a retention period for anonymized data, which creates opportunities for misuse. Other privacy safeguards provided by the GDPR are more abstract in nature but still significantly contribute to privacy protection by serving as a standardization source that allows unmanned aerial vehicle market participants to engage in targeted self-regulation. Thus, consent remains the cornerstone of the EU data protection regime. However, aside from some useful specific privacy protection measures set out in the GDPR, privacy protection based on the self-management privacy paradigm would be ineffective in the context of unmanned aerial vehicle use.

6. Privacy self-management based on individual consent has drawbacks. When giving consent for data processing, people often do not understand the real consequences of their choice or perceive them in a somewhat distorted manner due to their inherent limited rationality. It can also be argued that individuals in today's market conditions do not have real autonomy in making decisions, as business models that collect less data simply do not exist in the economy. Moreover, people do not have the time to read privacy policies or accurately anticipate the long-term consequences of data processing and its combination (aggregation). One solution proposed in academic literature is paternalistic regulation, which essentially restricts individual freedom of choice for their own well-being. Paternalistic provisions are abundant in various modern legal acts, including the GDPR and specialized drone regulations. The regulatory model for drones proposed by the author of the dissertation is also paternalistic. It is based not on consent but on mandatory behavioral rules established through formal regulation. The main aspect that makes this regulatory model appealing is its simplicity. Its implementation would ease the workload of courts and, through discussions on how privacy should be regulated in public spaces, would engage the broader public. According to the dissertation author, the proposed regulation could be implemented through formal regulation, regulation by informing, and standardization.

Further assessments by the dissertation author regarding issues related to the use of drones are provided in the dissertation itself.

Recommendations

1. EU Regulations No. 2019/945 and 2019/947 prescribe mandatory remote identification devices for many drones. Currently, the transmission of flight identification data is mandatory only locally (via radio communication), which complicates the detection of violations when drones are used for covert surveillance. A possible solution could be the transmission of identification data not only via radio communication but also via the internet to a central governmental authority. However, based on recent years' experience in the U.S., implementing this proposal at the moment would be challenging due to the insufficient development of remote identification technology. Therefore, EU legislators should take this proposal into account when preparing drone regulations in the future, as remote identification device technology becomes more advanced.

2. EU Regulations No. 2019/945 and 2019/947 prescribe the requirement to store records of drone flight operations. This measure could help ensure a certain level of privacy protection, but under the current EU regulation, the amount of data to be stored is insufficient to make it effective. The author recommends collecting more personal data to reconstruct the details of committed violations. When increasing the amount of data to be stored, the following conditions should be observed: 1) data should be stored only in the drone and not accessible via the internet (black box), 2) data should be provided to third parties only upon the legitimate request of an authorized governmental authority (e.g., court, pre-trial investigator, etc.), 3) a specific, limited data retention period should be established.

3. EU Regulations No. 2019/945 and 2019/947 prescribe that drones weighing less than 250 g are not required to have remote identification devices. In the future, privacy-related problems will primarily arise from small drones that, without remote identification devices, will remain unidentifiable to affected third parties or law enforcement authorities. Therefore, it is recommended to amend the EU's special drone regulation to require that remote identification devices be mandatory not only based on weight but also, analogously to the EU's drone registration provisions, based on the ability to collect personal data. The requirement for remote identification devices could also be linked to the registration requirement (i.e., if a drone must be registered, it should also have a remote identification device).

4. EU Regulations No. 2019/945 and 2019/947 prescribe the requirement to manufacture drones with lights. Current regulation makes an exception for drones weighing less than 250 g. However, even drones of such weight or lighter can infringe on privacy. In the future, small drones will make it even easier to violate privacy. Lights are one of the easiest, cheapest, and most effective measures to protect privacy. Therefore, the requirement to manufacture drones with lights should apply to all drones capable of capturing personal data, regardless of whether the

flight is conducted during the day or at night. To implement this proposal, it should be established that the light source of drones must be strong enough to be visible from a distance sufficient to effectively protect privacy and attract the attention of bystanders even on a sunny day.

5. When personal data is collected by a drone for commercial purposes, under EU legal regulations, the operator must obtain the consent of the data subjects before the flight. Before drones were introduced, consent was the most commonly used measure for self-managed privacy protection on the internet, but it is difficult to apply this measure to drones, as obtaining consent every time before a flight would be challenging for the operator. Due to the lack of an adapted legal framework, over time, this could become an obstacle to the technological advancement of drones. As a solution, the author recommends that in the future, lawmakers and courts adopt a paternalistic boundary management theory, which is based not on consent but on mandatory behavioral rules established through formal regulation.

6. Many of the anonymization technologies available today have inherent shortcomings, making it currently impossible to reliably anonymize data. Despite the fact that anonymized information can now be re-identified, legal regulations do not provide for retention periods for such data. This legal gap could be exploited by large data controllers, creating privacy threats through aggregation, security breaches, and identification violations. The author recommends establishing a retention period for anonymized data in legal regulations.

APPROVAL AND DISSEMINATION OF RESEARCH RESULTS

Part of the research conducted in the dissertation has been published in the scientific journals "Baltic Journal of Law & Politics" and "Teisės apžvalga" as well as the book „Future law, ethics, and smart technologies: the future of legal education":

Kiršienė, Julija, Christopher Kelley, Deividas Kiršys, and Juras Žymančius. "Rethinking the Implications of Transformative Economic Innovations: Mapping Challenges of Private Law." Baltic Journal of Law & Politics 12, no. 2 (2019): 47–77.

Kiršys, Deividas. "Drone threats to privacy: Possible infringements" Teisės apžvalga, no. 1 (2021): 64–87.

Kiršienė, J., Gruodytė, E., & Kiršys, D. (2023). Transformative Smart Technologies: Mapping Challenges of Private Law. In Future Law, Ethics, and Smart Technologies (pp. 30-47). Brill.

Part of the research results were also presented at scientific events:

On 20 February 2020, a presentation titled "Do drones infringe on our right to privacy?" was delivered at the international scientific conference "Future Law, Ethics, and Smart Technologies."

On 6 November 2020, a presentation titled "Does the use of drones violate the right to privacy?" was delivered at the workshops "Legal Issues in the Digital Society" organized by the Faculty of Law at Vytautas Magnus University.

CURRICULUM VITAE

Name: Deividas
Surname: Kiršys

Education

2017 – 2024	Mykolas Romeris University, Law School, doctoral studies
2015 – 2015	University of Luxembourg, ERASMUS student in the European Union Law Master's program
2011 – 2016	Vytautas Magnus University, Master's degree in Law
2011 – 2016	Michigan State University, Certificate in Transnational Law
2011 – 2016	Vytautas Magnus University, Supplementary studies in Political Science

Work experience

2023 – Now	Head of Legal & Compliance, UAB "TV Žaidimai"
2021 – 2022	Legal Officer, Citco Mercator, UAB
2020 – 2021	Assistant to an Attorney-at-Law, APB "Čerka ir partneriai"
2018 – 2021	Legal Counsel / Mediator, self-employment
2018 – 2020	Quasi-judge, Lithuanian Administrative Disputes Commission, Šiauliai Regional Branch
2016 – 2017	Legal Counsel, Šiaulių m. 4-asis notarų biuras
2015 – 2016	Legal Assistant, APB "Magnusson ir partneriai"

Other

2015 – 2016	Member of the Revision Commission, European Law Students' Association Lithuania Branch
2014 – 2015	President, European Law Students' Association Vytautas Magnus University Branch
2013 – 2014	Vice President of STEP, European Law Students' Association Vytautas Magnus University Branch

Deividas Kiršys
KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS: daktaro disertacija. – Vilnius: Mykolo Romerio universtitetas, 2025. P. 285.

Bibliogr. 196–211 p.

Bepiločių orlaivių naudojimas komerciniais tikslais kelia naujus iššūkius privatumo apsaugai, nes šios technologijos savybės – nepastebimumas, stebėjimo intensyvumas ir galimybė rinkti duomenis iš įvairių kampų – gali lemti masinę stebėseną ir privatumo pažeidimus. Ši disertacija analizuoja teisinius komercinių bepiločių orlaivių naudojimo aspektus, siekdama atskleisti, kaip suderinti technologinę pažangą su privatumo apsauga. Tyrimas apima ES, JAV ir tarptautinius teisės aktus, taip pat teismų praktiką, identifikuojant esamos teisinės bazės trūkumus. Disertacijoje atskleidžiama, kad dabartiniai teisės aktai nepakankamai reguliuoja privatumo apsaugą, ypač viešojoje erdvėje, kur bepiločiai orlaiviai gali būti naudojami slaptai stebėti asmenis. Tyrimas parodo, kad privatumo apsauga, paremta individo sutikimu, yra neveiksminga, nes žmonės dažnai nesupranta savo pasirinkimo pasekmių arba neturi realios galimybės atsisakyti duomenų rinkimo. Siekiant efektyvesnės privatumo apsaugos, disertacijoje siūlomas paternalistinis reguliavimo modelis, pagrįstas ribų valdymo teorija. Šis modelis leistų užtikrinti, kad privatumo apsauga nebūtų priklausoma nuo individo iniciatyvos, o būtų grindžiamas privalomomis elgesio taisyklėmis. Šis darbas yra reikšmingas mokslinis indėlis, kuris gali tapti pagrindu tolesniam teisiniam reguliavimui, teismų praktikai ir moksliniams tyrimams, susijusiems su naujų technologijų ir privatumo santykiu.

The use of commercial drones poses new challenges to privacy protection due to the unique characteristics of this technology, such as unobtrusiveness, intensive surveillance capabilities, and the ability to collect data from multiple angles, which can lead to mass monitoring and privacy violations. This dissertation examines the legal aspects of commercial drone usage, aiming to reconcile technological advancement with privacy protection. The study analyzes EU, U.S., and international regulations, as well as case law, identifying shortcomings in the current legal framework. The research reveals that current legislation inadequately addresses privacy concerns, particularly in public spaces, where drones can be used for covert surveillance. The study demonstrates that privacy protection based on individual consent is ineffective, as people often do not fully understand the consequences of their choices or lack the ability to refuse data collection. To ensure more effective privacy protection, the author proposes a paternalistic regulatory model based on boundary management theory.

This model would shift the focus from individual consent to mandatory behavioral rules, ensuring that privacy protection does not rely solely on individual initiative. This research represents a significant academic contribution and can serve as a foundation for future legal regulation, judicial practice, and scholarly studies on the relationship between emerging technologies and privacy.

Deividas Kiršys

KOMERCINIŲ BEPILOČIŲ ORLAIVIŲ NAUDOJIMAS IR PRIVATUMO APSAUGA: TEISINIAI IŠŠŪKIAI IR REGULIAVIMO TOBULINIMO GAIRĖS

Daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai Raimonda Smailytė

Spausdino UAB „Šiaulių spaustuvė“
P. Lukšio g. 9G, 76200 Šiauliai
El. p. info@dailu.lt
https://siauliuspaustuve.lt