VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

# DRONŲ GRĖSMĖ PRIVATUMUI: GALIMI PAŽEIDIMAI

Deividas Kiršys[1]
DOI: https://doi.org/10.7220/2029-4239.23.4

## SANTRAUKA

*Šiame straipsnyje siekiama atskleisti, kokius privatumo pažeidimus gali sukelti nedidelių bepiločių orlaivių (taip pat žinomų kaip dronai ar UAS) naudojimas. Moksliniame diskurse dažnai pripažįstama, kad UAS kelia grėsmę privatumui, tačiau akademikai, priimdami tokią išvadą, potencialų pavojų tiesiog preziumuoja, apsiribodami vienu ar keliais pavyzdžiais, tačiau plačiau privatumo pažeidimų, kuriuos gali sukelti dronų naudojimas, išsamiai neaptaria. Straipsnyje, vadovaujantis Daniel Solove pažeidimų taksonomija, parodoma, kad dronų naudojimas teisę į privatumą pažeidžia visokiais būdais. UAS gali būti įvairių dydžių ir konfigūracijų, todėl yra tobulos informacijos rinkimo priemonės, galinčios įrašyti ne tik vaizdą, bet ir garsą, užfiksuoti šilumos pakitimus aplinkoje, aptikti cheminius pėdsakus, fiksuoti bevielį duomenų srautą. Tiek valstybės, tiek privatūs subjektai gali norėti pasinaudoti šia technologija, siekdamos sukurti sistemingos ir plataus masto stebėsenos infrastruktūrą, kuri ilgainiui visuomenėje gali sukelti atšalimo efektą. Dronų derinimas su milžiniškomis duomenų bazėmis bei agregavimo programine įranga gali lemti labai nevienodą galios pasiskirstymą visuomenėje, nes galingi subjektai gali būti linkę turimais duomenimis piktnaudžiauti, taip pat sukuria erdvę klaidingai individų elgesio interpretacijai, išankstiniams nusistatymams. Bepiločiai orlaiviai gali būti derinami su veido atpažinimo programine įranga, kuri suteiks galimybę susieti realius žmones su jų profiliais elektroninėje erdvėje. Susirūpinimą taip pat kelia surinktų duomenų saugumas bei UAS neatsparumas kibernetinėms atakoms, bei jų, kaip įrankių kibernetinėms atakoms vykdyti, naudojimas. Be sisteminių problemų, dronų gebėjimas prie stebimojo priskristi bet kokiu kampu, sukuria dingstis dažnesniems vojerizmo išpuoliams. Straipnyje prieinama išvada, kad bepiločiai orlaiviai yra rimta grėsmė privatumui bei nurodomos pagrindinės priežastys, kodėl dabartinis reguliavimas gali būti nepakankamas siekiant pažaboti su dronų naudojimu susijusias grėsmes.*

[1] Autorius yra Mykolo Romerio universiteto su Vytauto Didžiojo universitetu teisės mokslo krypties doktorantas.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

# REIKŠMINIAI ŽODŽIAI

*Dronai, bepiločiai orlaiviai, UAS, privatumas, pažeidimai, klasifikacija, taksonomija.*

# ĮVADAS

Per pastarąjį dešimtmetį nedidelių bepiločių orlaivių, populiariai žinomų kaip dronai arba UAS[2], naudojimas stebėtinai išaugo. Nors dronai anksčiau buvo naudojami tiktai kariniais tikslais, šiais laikais, kai šie skraidantys robotai prieinami plačiajai visuomenei, dronų panaudojimo būdų sąrašas kasdien pasipildo. Bepiločiai orlaiviai gali būti įvairių dydžių – nuo tokių mažų kaip vabzdys iki tokių, kurie panašesni į tradicinius pilotuojamus orlaivius. Kol kas UAS gali būti naudojami siuntinių pristatymui, detalių žemėlapių sudarymui, gelbėjimo operacijų vykdymui, įrodymų rinkimui, fotografijai. Praktiškai kiekvienas dronas yra „apginkluotas“ bent jau patenkinamos kokybės vaizdą sugebančia atkurti vaizdo kamera, o kai kurie ir itin aukštos raiškos profesionalia filmavimo įranga, kryptiniais mikrofonais, bevielių ryšių imtuvais, vietos nustatymo sistemomis, RFID sensoriais, adaptyvia programine įranga, kurią galima panaudoti veidų atpažinimui, tapatybės nustatymui. Galimybė prie dronų pritaisyti įvairius papildomus komponentus ir juos rotorių pagalba pakelti į orą suteikia dronams revoliucinio duomenų rinkimo prietaiso statusą. Kaip ir atsiradus kibernetinei erdvei[3], taip ir atsiradus UAS, tokia patogia duomenų rinkimo platforma anksčiau ar vėliau gali norėti pasinaudoti ne tik valstybės ar tarptautinės komercinės korporacijos, tačiau ir duomenis iš pagrindinių duomenų rinkėjų sugebantys pavogti programišiai, nusikalstamos ar teroristinės organizacijos. Tikrosios dronų panaudojimo galimybės bus išnaudotos tuomet, kai jie taps iš dalies arba visiškai autonomiškai valdomi, kadangi sistemingam sekimui vykdyti užteks interneto ir pažangių algoritmų, o žmogiškųjų išteklių reikės minimalių arba nebereikės iš viso.

Daugelis pripažįsta, kad bepiločiai orlaiviai kelia grėsmę privatumui[4]. Vis dėlto, siekdami parodyti, konkrečiai kokiais būdais teisė į privatumą pažeidžiama, mokslininkai dažnai

[2] Europos Sąjungos dokumentuose bepiločio orlaivio sistema (UAS) apibūdinama kaip bepilotis orlaivis ir jo nuotolinio valdymo įranga, žr.: „2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos“, OL L 152, 2019-06-11, p. 45—71.

[3] Dauguma interneto vartotojų šiais laikais puikiai supranta, kad viską, ką jie pasisako ar atlieka internete, stebi ir seka įvairūs subjektai nuo pardavėjų ir reklamuotojų iki valstybės institucijų ir internetinių persekiotojų, nusikalstamų organizacijų, žr.: Joan Feigenbaum ir Bryan Ford, „Seeking Anonymity in an Internet Panopticon“, *Commun. ACM* 58, Nr. 10 (2015 m.), p. 58–69, https://doi.org/10.1145/2714561.

[4] Žr. pvz.: Aurelija Pūraitė, Daiva Bereikienė, ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania“, *Baltic Journal of Law & Politics* 10, nr. 2 (2017 m.): 107–32, M. Ryan Calo, „The Drone as a Privacy Catalyst“, *Stanford Law Review Online* 64 (2011 m.), p. 29–33; Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy“, *Technology in Society* 46 (2016 m. rugpjūčio 1 d.), p. 109–19, https://doi.org/10.1016/j.techsoc.2016.03.003; Rachel L. Finn ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications“, *Computer Law & Security Review* 28, Nr. 2 (2012 m. balandžio 1 d.), p. 184–94, https://doi.org/10.1016/j.clsr.2012.01.005; Paul McBride, „Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations Comment“, *Journal of Air Law and Commerce* 74 (2009 m.), p. 627–62; Uri Volovelsky, „Civilian uses of unmanned

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

apsiriboja vienu ar keliais pavyzdžiais. Kitaip tariant, neretai pripažįstama, jog grėsmė egzistuoja, tačiau konkretūs privatumo pažeidimai, kuriuos gali sukelti dronų naudojimas, išsamiai neaptariami. Iš to kyla susijusi problema: kol neidentifikuoti realūs privatumo pažeidimai, sudėtinga įsivaizduoti, kokių priemonių reikėtų imtis, kad jų būtų išvengta ateityje. Šiuo straipsniu siekiama identifikuoti, kokias konkrečias grėsmes dronai kelia privatumui, tokiu būdu užpildant spragą mokslinėje literatūroje ir suteikiant aiškų pagrindą tolesniems dronų privatumo reguliavimo tyrimams.

Šis straipsnis suskirstytas į tris dalis. Pirma dalis skirta aptarti metodologijai, kuria vadovaujamasi siekiant įvykdyti straipsnyje išsikeltą tikslą. Antroje dalyje identifikuojami ir nuodugniai aptariami konkretūs privatumo pažeidimai, kuriuos gali sukelti nedidelių dronų naudojimas. Trečioje dalyje pateikiamos išvados ir įžvalgos padėsiančios tolesniems tyrimams UAS ir privatumo tematika.

# METODOLOGIJA

Apibrėžti, kas yra teisė į privatumą, gali būti sudėtinga, tačiau akademikai yra sukūrę kelis metodologinius lęšius, kurie palengvina šios teisės suvokimą. Autorius galima suskirstyti į dvi pagrindines stovyklas: tuos, kurie teisę į privatumą suskirsto į vertybines dimensijas[5], bei tuos, kurie privatumą klasifikuoja pagal pažeidimus[6]. Pirmosios stovyklos klasifikacijos labiau abstrakčios, t. y. labiau tinka bendriems teisinio reguliavimo tikslams išsikelti, negu identifikuoti vyraujančias problemas. Antrosios grupės klasifikacijos yra labiau pragmatiškos, t. y. padeda vaizdingiau atkurti praktines situacijas, kylančias iš dronų naudojimo, todėl leidžia aiškiau parodyti, kokią grėsmę nedidelių dronų naudojimas gali kelti privatumui. Norint aiškiai ir nedviprasmiškai atskleisti dronų keliamą grėsmę privatumui, mano nuomone, geriausiai tinka antrosios grupės atstovo sukurta privatumo pažeidimų klasifikacija[7], kuri apibendrinama žemiau atvaizduotoje Schemoje Nr. 1. Būtent ji ir bus šio straipsnio metodologinis pagrindas.

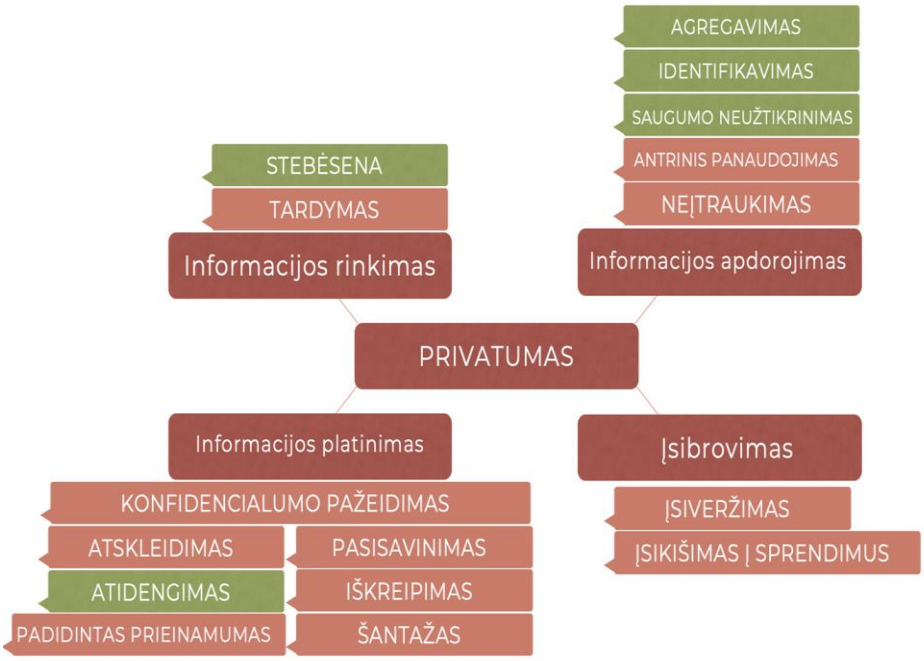
aerial vehicles and the threat to the right to privacy – An Israeli case study“, *Computer Law & Security Review* 30, Nr. 3 (2014 m. birželio 1 d.), p. 306–20, https://doi.org/10.1016/j.clsr.2014.03.008; Roger Clarke, „The regulation of civilian drones' impacts on behavioural privacy“, Computer Law & Security Review 30, Nr. 3 (2014 m. birželio 1 d.), p. 286–305, https://doi.org/10.1016/j.clsr.2014.03.005; 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), t. 4 (IEEE, 2015 m.), p. 1–6; Jonathan P. West ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues“, Public Administration Review 76, Nr. 4 (2016 m.), p. 649–659.

[5] Žr. pvz. Rachel L. Finn, David Wright, ir Michael Friedewald, „Seven types of privacy“, European data protection: coming of age (Springer, 2013), 3–32; Roger Clarke, Introduction to dataveillance and information privacy (Australian National University, 2006).

[6] Daniel J. Solove, „A Taxonomy of Privacy“, University of Pennsylvania Law Review 154, nr. 3 (2005 m. 2006): 477–564; Debbie V. S. Kasper, „The evolution (or devolution) of privacy“, Sociological Forum, t. 20 (Springer, 2005), 69–92.

[7] Žr. išnaša Nr. 6: Daniel J. Solove, „A Taxonomy of Privacy“.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*




Schema Nr. 1: Privatumo pažeidimų klasifikacija

# PAŽEIDIMAI, KURIUOS GALI SUKELTI NEDIDELIŲ DRONŲ NAUDOJIMAS

Šiame skyriuje vadovaujantis schemoje pavaizduota privatumo pažeidimų klasifikacija bus konkrečiau identifikuoti pažeidimai, kurie gali iškilti didėjant nedidelių dronų pritaikymo galimybėms. Natūralu, kad dronai nesukelia absoliučiai visų klasifikacijoje nurodytų pažeidimų, todėl toliau plačiau atskleidžiamos tik tos grėsmės, kurios labiausiai susijusios su dronų naudojimu, tokios yra, mano nuomone, stebėsena, agregavimas, identifikavimas, saugumo neužtikrinimas ir atidengimas (Schemoje Nr. 1 pažymėtos žaliai).

## Stebėsena

Nedideli dronai išsiskiria skrydžio kontrolės paprastumu ir gebėjimu fiksuoti vaizdus. Technologijoms tobulėjant, tikėtina, jog nedideli UAS per didelį atstumą arba vabzdžio dydžio bepiločiai orlaiviai iš labai arti galės įrašyti ne tik vaizdą, bet ir garsą, užfiksuoti šilumos

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

pakitimus aplinkoje, aptikti cheminius pėdsakus[8], fiksuoti bevielį duomenų srautą[9]. Dėl šių techninių galimybių privatumo teisės kontekste dronai, pirmiausia, yra informacijos rinkimo priemonės, todėl patenka į Schemoje Nr. 1 įvardintą *informacijos rinkimo* pažeidimų kategoriją. Iš dviejų šios kategorijos privatumo pažeidimo rūšių, bepiločiams orlaiviams tinka viena – *stebėsena*. Jie gali būti panaudojami žmonių stebėjimui (darant vaizdo ar garso įrašus), šiems apie tai nežinant arba tik numanant, kad yra stebimi. Be abejo, kol technologinės galimybės leidžia dronus valdyti tik nuotoliniu būdu, plataus masto sekimas reikalautų ypatingai didelių žmogiškųjų išteklių, tačiau didėjant šių skraidančių pagalbininkų autonomijai, galimybė pasirinktą asmenį stebėti nuolatos, galiausiai, taps nebe mokslinės fantastikos sritis.

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 resursus, tačiau iš jų tik valstybės turi tokius plačius įgaliojimus vykdyti sistemingą ir plataus masto stebėseną. Skiriasi ir šių subjektų motyvacija – privačių įmonių vykdomos stebėsenos tikslas yra padidinti parduodamų produktų ar paslaugų paklausą, tuo tarpu valstybių sumanymai panaudoti surinktą informaciją gali būti kur kas ambicingesni ir gali sukelti žymiai didesnių neigiamų pasekmių[10]. Negana to, valstybės gali naudotis privačių subjektų sukurta stebėsenos infrastruktūra teisės aktuose nustatydamos reikalavimą kaupti surinktą informaciją ir, esant reikalui, suteikti prieigą valdžios institucijoms[11], ar nustatydamos reikalavimą surinktą informaciją iš karto perduoti valdžios institucijoms. Kita vertus, ar blogai, kad valstybė kaupia informaciją siekdama apsaugoti savo piliečius? Ar nelogiška atiduoti dalį savo privatumo vardan 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 žvalgybą – kuo didesnė ir kuo turtingesnė valstybė, tuo platesnis jos žvalgybos tinklas. Pavyzdžiui, Edward Snowden skandalas[12] parodė, jog didžiausios ir galingiausios pasaulio valstybės gali į asmenų gyvenimus įsibrauti net ir pačiomis netikėčiausiomis priemonėmis. Be abejonės, daugelį individų tokio masto sekimas priverčia jaustis nepatogiai, tačiau valstybės atkerta gana įtikinamu teiginiu: „nėra ko bijoti, jeigu

[8] 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/.

[9] Vienas iš mažiau žinomų faktų apie stebėjimui ir kariniams tikslams naudojamus bepiločius orlaivius yra tai, kad be ginklų, kamerų ir kitų jutiklių jie aprūpinti dar ir įrenginiu, vadinamu„ Air Handler“, kuris gali užfiksuoti visą aplinkinį belaidį duomenų srautą, žr.: Mark Andrejevic ir Kelly Gates, „Big Data Surveillance: Introduction“, *Surveillance & Society* 12, Nr. 2 (2014 m. gegužės 9 d.), p. 185–96, https://doi.org/10.24908/ss.v12i2.5242.

[10] Užtenka prisiminti ambicingą nacistinės Vokietijos siekį sukurti fiurerio Adolfo Hitlerio valdomą naują, harmoningą visuomenę, kuris baigėsi beveik šešių milijonų žydų žūtimi.

[11] Pavyzdžiui, 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.

[12] Edward Snowden, buvęs CŽV darbuotojas, 2013 metų 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.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

neturi, ko slėpti“[13]. Ir iš tiesų, kodėl valstybės vykdoma stebėsena turėtų būti laikoma privatumo pažeidimu, jeigu dauguma surinktos informacijos nėra jautri, bet kokia informacija yra atskleidžiama tik tuo atveju, jeigu išaiškinamas nusikaltimas, o asmenys, bandę nuslėpti nusikalstamą veiką, neturi jokios pagrįstos teisės išsaugoti nusikalstamos veikos privatumą. Be to, dronai neužilgo gebės informaciją rinkti autonomiškai, surinktus duomenis tikriausiai apdoros kompiuteriai, todėl, jeigu asmuo neslėptų jokios nusikalstamos veikos, kompiuteris, neužfiksavęs jokių įtartinų veiksmų, surinktą informaciją tiesiog abejingai praleistų, o nufilmuoti vaizdai niekada taip ir nepasiektų valstybės pareigūnų akių. Vadovaujantis šiuo argumentu, piliečiams, kurie pavyzdingai laikosi įstatymų, dėl savo privatumo bijoti nereikia, nes valstybei yra įdomūs tiktai asmenys, kurie daro nusikaltimus.

Vis dėlto, „neturiu ko slėpti“ argumentu daroma trumparegiška prielaida, kad privatumo esmė yra kažko blogo nuslėpimas nuo trečiųjų asmenų. Priešingai, privatumas susideda iš daugybės vertybinių elementų, kurių kiekvienas turi tam tikrą socialinę reikšmę, o kažko blogo nuslėpimas nuo visuomenės galėtų būti tiktai smulkus visos privatumo koncepcijos elementas. Nors bet kokia nuolatinė žmogaus stebėsena jau gali būti traktuojama kaip privatumo pažeidimas, žmonių elgesio pokyčiai dar savaime nėra blogas dalykas ir gali turėti tam tikros visuomeninės naudos, pavyzdžiui, tam tikras socialinės kontrolės lygis, kaip antai, viešų erdvių stebėjimas šiais laikais plačiai naudojamomis vaizdo stebėjimo kameromis (CCTV) gali prislopinti žmonių elgesį, kuris yra nelegalus ar visuomenės smerktinas. Tačiau per didelis socialinės kontrolės lygis, pavyzdžiui, slapta stebėsena filmuojant vabzdžio dydžio dronais iš arti arba iš tokio didelio atstumo, kad dronas plika akimi neįžiūrimas ir negirdimas, gali neigiamai paveikti individų laisvės pojūtį, kūrybingumą, saviugdą, priversti jaustis nepatogiai, sukelti elgesio pakitimus, nes stebimi žmonės jaučiasi labiau suvaržyti bei labiau laikosi įprastų socialinių normų [14]. Mokslininkai šią stebėsenos sukeltą visuomenės savidiscipliną vadina *atšalimo* arba *panoptiniu efektu*[15].

Slapta stebėsena pažeidžia asmens privatumo teisę ne tik tada, kai asmuo yra privačioje aplinkoje, pvz. savo bute, name, žemės sklype, bet ir tuomet, kai yra viešoje erdvėje, tačiau gali pagrįstai tikėtis, jog tuo metu nėra stebimas, pavyzdžiui, būdamas tyliame viešo parko kampelyje, tankioje ir triukšmingoje minioje sporto renginyje ir panašiai. Be abejo, asmuo gali tikėtis, jog viešoje vietoje atsitiktinai pateks į nuotrauką ar vaizdo įrašą, kuriame yra ir kitų žmonių, tačiau negali iš anksto numanyti, kad nuotraukoje ar vaizdo įraše bus tikslingai pritrauktas iš arti arba bus pasiklausomas kryptiniu mikrofonu.[16] Nors priimta manyti, jog viešoje vietoje asmuo negali tikėtis privatumo[17], tačiau tokio masto stebėjimas, kokį įgalina dronų technologijos, netgi ir

[13] Daniel J. Solove, „I’ve Got Nothing to Hide and Other Misunderstandings of Privacy 2007 Editor’s Symposium“, *San Diego Law Review* 44 (2007 m.), p. 748.

[14] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 493 - 494.

[15] Terminas „panoptinis“ yra kilęs Jeremy Bentham aprašyto utopinio kalėjimo, jo knygoje vadinamo „Panoptikumu“, kurio architektūriniai sprendimai turėjo sudaryti galimybę apsaugai stebėti kalinius šiems žinant, kad bet kada *gali* būti stebimi, tačiau tiksliai niekada nežinant ar konkrečiu momentu *yra* stebimi. Jeremy Bentham, Panopticon Or the Inspection House (T. Payne, 1791).

[16] Žr. išnaša Nr. 4: Clarke, „The regulation of civilian drones’ impacts on behavioural privacy,“ p. 288.

[17] Pavyzdžiui, LR CPK 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. Lietuvos Respublikos Civilinio proceso kodeksas (suvestinė redakcija nuo 2020-07-09), *Žin.* (2002-04-06, Nr. 36-

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

viešoje vietoje gali pažeisti asmens teisę į privatumą. Iki šiol viešoje vietoje kažką sekti jam to nežinant buvo pernelyg sudėtinga arba reikalavo pernelyg didelių išteklių, vis dėlto, dronų technologijos suteikia galimybę individą stebėti bet kokiu pageidaujamu kampu bei ženkliai sumažinti kaštus, reikalingus sistemingai ir nuolatinei stebėsenai. Pastovi individo stebėsena viešoje vietoje gali pažeisti teisę į privatumą dar daugiau negu stebėsena privačioje erdvėje, kadangi tai, kur asmuo eina ir su kuo kontaktuoja viešoje erdvėje gali pasakyti kur kas daugiau apie individo gyvenimą, negu tai, kada ir ką jis darosi valgyti, kada žiūri mėgstamą serialą, kokią knygą skaito prieš miegą ir panašiai.

Asmens privatumas gali būti pažeidžiamas net ir tada, kai konkretus asmuo nėra sistemiškai sekamas ir nėra pagrindinis sekimo objektas. Kai pagrindinis sekimo tikslas tampa surinkti kiek įmanoma daugiau informacijos apie bet ką ir amžinai šią informaciją talpinti laikmenose, nebereikia stebėti konkrečių individų, galima tiesiog stebėti visus ir visada, o reikiamą informaciją išgauti tik tuomet, kai jos reikia [18]. Tokiems dideliems surinktos informacijos kiekiams apdoroti jau nebeužtektų net ir visos armijos žmonių, todėl į pagalbą pasitelkiamos kompiuterinės programos, kurios pagal užprogramuotus algoritmus surinktoje medžiagoje atranda veiksmų šablonus, atpažįsta veidus, konkrečius žodžius ir panašiai. Nors didžiosios dalies surinktos informacijos tokiu atveju žmonių akys neišvystų, esant reikalui ji galėtų būti panaudota prieš pačius stebimuosius siekiant įgyti kokį nors pranašumą. Apie tai, kaip privatumas gali būti pažeidžiamas jau surinkus didelį kiekį informacijos, plačiau bus aptariama toliau kitame šio straipsnio skyriuje analizuojant dar vieną privatumo pažeidimą, susijusį su padidėjusiu nedidelių dronų prieinamumu – agregavimą.

## Agregavimas

Dronai nuolatos apdoroja surinktą informaciją, naudodami programinę įrangą, kuri padeda informaciją perkelti į laikmeną, perduoti duomenis duomenų ryšiu, atkurti filmuojamą vaizdą valdymo pulto ekrane ir pan., todėl dronais turėtų būti įmanoma įvykdyti privatumo pažeidimus, įvardytus D. Solove klasifikacijos *informacijos apdorojimo* kategorijoje (žr. Lentelę Nr. 1).

Jeigu anksčiau buvo praktinių apribojimų, neleidžiančių vienu metu sekti milijonų žmonių judėjimą dideliame mieste (reikėtų milžiniškų lėšų pasamdyti pakankamai agentų, kurie sektų milijonams žmonių iš paskos ir užsirašinėtų pastabas), šiandien įžiūrėti naudingą, tačiau neakivaizdžią žmonių elgesio struktūrą, mums gali padėti technologijos, tarp jų ir bepiločiai orlaiviai. Žmonės tiesiog fiziškai nesugebėtų atlikti tokio masto duomenų analizės be pagalbos. Pasitelkiant dronus galima surinkti labai didelius informacijos kiekius, o surinkti duomenys pasitelkiant pažangią programinę įrangą vėliau gali būti tarpusavyje derinami bei interpretuojami. Šis privatumo pažeidimas D. Solove įvardijamas kaip *agregavimas*.

Kaip ir stebėsena, agregavimas yra būdas surinkti informaciją apie žmones, tačiau labiau netiesioginiu būdu – apdorojant jau surinktą informaciją. Dronai informacijos apdorojimo procese dalyvauja labai nedaug, kadangi jų pagrindinė užduotis yra informaciją surinkti ir perduoti į duomenų bazę, kurioje programinė įranga toliau atlieka rūšiavimo ir interpretavimo darbus. Vis dėlto UAS prie šio pažeidimo tipo prisideda reikšmingai, nes įgalina oportunistinį,

1340 ). Analogišką problemą D. Solove įžvelgia ir JAV privatumo reglamentavime, žr. išnaša Nr. 10: Solove, „A Taxonomy of Privacy,“ p. 498.

[18] Žr. išnaša Nr. 9: Andrejevic ir Gates, „Big Data Surveillance,“ p. 185.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

visur esantį informacijos rinkimą[19]. Tokio plataus masto informacijos rinkimas ir apdorojimas, kurio tikslas sužinoti ne ką nors konkretaus apie konkretų asmenį, bet veikiau sužinoti kuo daugiau ir bet kokios informacijos apie visus įmanomus asmenis, yra vadinamas populiariu terminu „didieji duomenys“ (angl. „Big data“). Įvairiais sensoriais aprūpinti dronai yra pajėgūs užfiksuoti ne tik didelius kiekius vaizdų, garsų, bet ir visur sklindantį duomenų ryšį (Wi-Fi, 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[20], bet ir duomenis apie tai, kaip mes elgiamės realiame gyvenime. Surinkti duomenys galės būti panaudojami daugeliui gerų tikslų, pavyzdžiui, ligų paplitimo įvertinimui, verslo tendencijų sekimui, organizuoto nusikalstamumo išaiškinimui, interneto srauto analizei bei įvairioms prognozėms nuo orų iki finansinių rinkų[21].

Vis dėlto dronų derinimas su milžiniškomis duomenų bazėmis bei agregavimo programine įranga gali suteikti didžiųjų duomenų valdytojams akivaizdžių dingsčių savo padėtimi piktnaudžiauti. Agregavimas gali sukelti grėsmių privatumui dėl to, kad gali apie žmogų atskleisti tokių dalykų, kurių asmuo nesitikėjo atskleisti. Asmuo savo kasdieniniame gyvenime per įvairius užsiėmimus pasirinktinai skleidžia mažas daleles duomenų ir pagrįstai tikisi, kad šios dalelės mažai ką pasakys apie jo asmeninį gyvenimą. Vis dėlto, kai visos duomenų dalelės būna konsoliduojamos, agreguotojas sužino kur kas daugiau apie individo asmeninį gyvenimą negu individas galėjo įsivaizduoti[22]. Šį teiginį puikiai iliustruoja tarptautinių parduotuvių tinklo „Target“ didžiųjų duomenų naudojimo pavyzdys. Netgi plačiausia reklaminė kampanija gali nepadėti pirkėją pervilioti iš vienos parduotuvės į kitą, tačiau, regis, lengviausias būdas tai padaryti yra, kai pirkėjo gyvenime vyksta radikalūs pokyčiai, vienas iš tokių – vaiko gimimas. Kadangi JAV gimimo įrašai dažniausiai yra vieši, „Target“ ir kiti parduotuvių tinklai šeimoms, kurios neseniai susilaukė vaiko, siųsdavo kuponus ir reklamas kūdikių prekėms įsigyti. Vis dėlto „Target“ nusprendė pabandyti šeimas pasiekti pirmi, kol dar mamos yra besilaukiančios, ir taip pralenkti savo konkurentus. Vienintelis klausimas buvo, kaip nustatyti, kad tam tikra moteris yra nėščia. Į pagalbą šiuo klausimu atėjo didieji duomenys[23]. Kompanija jau ir taip turėjo milžinišką vidinę duomenų bazę su klientų įsigyjamomis prekėmis. Lygindamas įsigyjamų pirkinių duomenis su viešais gimimo įrašais parduotuvių tinklas sugebėjo sudaryti pagrindinių prekių, kurias šeimos yra linkusios įsigyti prieš gimstant vaikui, tokių kaip bekvapis kūdikių kremas, kalcio papildai ir dezinfekcinės priemonės. Beliko šį standartinį nėščios moters profilį pritaikyti jau esamai pirkėjų duomenų bazei. Kaskart, kai moteris įsigydavo daugelį iš sąraše esančių produktų, „Target“ jai priskirdavo didelį prognozuojamo nėštumo balą ir siųsdavo jai su kūdikiais susijusių produktų reklamas ir kuponus. Kompanijai pradėjus vykdyti tokią reklamos strategiją po kelių mėnesių į vieną iš parduotuvių atėjo vyras skųsdamasis, 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

[19] Ten pat.

[20] 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.

[21] Žr. išnaša Nr. 9: Andrejevic ir Gates, „Big Data Surveillance,“ p. 186.

[22] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 508.

[23] Dennis D Hirsch, „That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority“, *Kentucky Law Journal* 103 (2014 m.), p. 350.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

ir vyras išėjo. Netrukus po incidento, vadybininkas dar kartą paskambino vyrui, kad jo atsiprašytų, tačiau prieš tai pasipiktinęs tėvas šį kartą jau buvo susigėdęs ir pats atsiprašinėjo vadybininko. Paaiškėjo, jog vyras pasikalbėjo su savo dukra ir sužinojo, jog ši iš tikrųjų buvo nėščia. „Target“ apie tai sužinojo pirmiau negu merginos tėvas[24]. Jeigu „Target“ iš klientės perkamų prekių sugebėjo nuspėti jos nėštumą, įsivaizduokite, kokius dalykus apie žmones dronų pagalba galėtų sužinoti ir kokių veiksmų imtis ambicingi Kinijos biurokratai[25].

Dronų technologijoms tobulėjant, tik laiko klausimas, kada didelę galią turintys subjektai, tarp jų ir šioje srityje pirmaujanti Kinija, žmones pradės stebėti visur ir visada. Viešoje erdvėje asmuo, prasilenkdamas su kitais praeiviais, pagrįstai tikisi, kad praeiviai nugirs kai kuriuos jo žodžius, pastebės kai kurias jo veido mimikas, pastebės, su kokiais žmonėmis jis tuo metu bendravo, tačiau kažin ar įsivaizduoja, kad tokią, iš pirmos pažiūros nieko nepasakančią informaciją, dronais renkant kiekvieną jo gyvenimo viešoje erdvėje minutę bei dedant į didelę duomenų bazę, programinė įranga gali įžvelgti žmogaus elgesio struktūras, kurių net pats žmogus nepastebėjo.

Kita agregavimo grėsmė yra susijusi su galios pasiskirstymu visuomenėje. Įprasta valdžios institucijų vykdoma stebėsena būna selektyvi, t. y. dažniausiai būna sekamas konkretus asmuo (įtariamasis), galimai susijęs su kokiu nors nusikaltimu. Tuo tarpu didieji duomenys visiškai pakeičia stebimojo (įtariamojo) sąvoką, kadangi stebėjimo taikiniais tampa nebe konkretūs individai ar įvykiai, o duomenyse paslėptos elgesio struktūros[26]. Didžiųjų duomenų stebėjimo esmė yra susemti kaip įmanoma daugiau informacijos ir tik vėliau išrūšiuoti, kuri informacija gali būti naudinga, todėl, kaip teigia M. Andrejevic ir K. Gates, pasitelkiant didžiuosius duomenis dažniausiai nėra bandoma paaiškinti ar suprasti pasaulį, kurį užfiksuoja duomenys. Tokio stebėjimo tikslas yra *įsikišti* į pasaulį per elgesio struktūras, kurias gali pastebėti tiktai turintys priėjimą ir galimybę didžiuosius duomenis apdoroti. Didžiųjų duomenų pasaulyje nebelieka jokio funkcinio skirtumo tarp įtariamųjų ir neįtariamųjų: tam, kad tarp jų galima būtų įžiūrėti reikšmingesnių skirtumų, reikalinga tampa informacija tiek apie vienus, tiek apie kitus[27]. Kaupiant informaciją tokiu būdu, kaip pastebi J. Packer, visa realybė yra išverčiama į skaitmeninius duomenis, dėl to visas pasaulis per skaitmeninę manipuliaciją gali būti transformuojamas[28]. Jeigu vien socialiniuose tinkluose surinkta informacija gali lemti JAV prezidento rinkimų rezultatus[29], socialinės kontrolės mastas, kuris gali būti pasiektas informaciją renkant dronais, tikriausiai netoli nukryptų nuo George Orwell vaizduojamo totalitarizmo[30]. K.

[24] Ten pat, p. 350–51.

[25] Dar 2018 metais internetinėje erdvėje pasirodė naujienų straipsniai, kuriuose teigiamas, kad Kinija testuoja į balandžius panašius dronus, kuriuos planuoja naudoti Kinijos populiacijos stebėjimui, žr. pvz.: Cristina Fernández Esteban, „China is testing creepy drones that look and fly like real birds to monitor citizens“, Business Insider, žiūrėta 2020 m. rugpjūčio 24 d., https://www.businessinsider.com/china-is-testing-creepy-dove-drones-to-monitor-citizens-2018-6.

[26] Žr. išnaša Nr. 9: Andrejevic ir Gates, „Big Data Surveillance,“ p. 190.

[27] Ten pat.

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

[29] 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.

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

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

D. Haggerty ir R. V. Ericson manymu, dabartinės stebėjimo technologijų galimybės netgi pranoko Orwell‘o distopinę viziją, viena, dėl to, kad Orwell‘o romane nuolatinį stebėjimą vykdė tik valstybės institucijos, tuo tarpu šiais laikais visuomenę masiškai stebi ne tik valstybė, bet ir nevalstybinės institucijos, antra, dėl to, kad Orwell‘o prognozėse „proliai“ turėtų būti didžiąja dalimi atleidžiami nuo stebėjimo, tačiau šiais laikais, panašu, kad stebima visa visuomenė be išimčių[31].

Dar viena agregavimo grėsmė yra susijusi su surinktų duomenų patikimumu. Didieji duomenys yra neišvengiamai priklausomi nuo infrastruktūros, kuri įgalina informaciją surinkti, talpinti ir apdoroti. Bet koks sistemos netobulumas yra kompensuojamas surinktų duomenų kiekiu, t. y. kuo daugiau informacijos duomenų bazėje, tuo patikimesnės išvados. Svarbiausia stadija šiame procese yra informacijos surinkimas, kadangi nuo surinktų duomenų kiekio ir objektyvumo priklauso, kiek patikimos bus algoritmų sugeneruotos išvados. Be abejo, duomenų surinkimo galimybes reikšmingai praplečia dronų technologija, kadangi ji įgalina įvairiais kampais informaciją rinkti realioje erdvėje, tačiau net ir tai neužtikrina išvadų patikimumo. Kaip teigia M. Andrejevic ir K. Gates, vien duomenų bazės dydis neužkerta kelio sistemiškų šališkumo formų atsiradimui duomenų bazėje arba algoritmuose, kurie ją rūšiuoja, vienintelis būdas nieko nepražiūrėti yra visiškai atgaminti pasaulį įrašytų duomenų forma bei rinkti duomenis apie patį duomenų rinkimo procesą ir taip toliau iki begalybės[32]. Kitaip tariant, kad ir kiek bandytume duomenų užfiksuoti, šie duomenys būtų tiktai realybės mėginys, kuris ne visuomet atspindėtų pačią realybę. 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[33]. Šis sistemos netobulumas yra grėsmė privatumui, nes sukuria erdvę klaidingai individų elgesio interpretacijai.

D. D. Hirsch kaip pavyzdį pateikia duomenų analitikų ir sveikatos priežiūros specialistų bendrą iniciatyvą, kurios tikslas visuomenėje atpažinti individus, kurie rizikuoja susirgti diabetu, ir šiems individams suteikti prevencinę priežiūrą[34]. Viena vertus, tokie duomenys medikų rankose galėtų išgelbėti daugybę gyvybių, tačiau kita vertus, jeigu prie šių duomenų taip pat galėtų prieiti bankai ar kitos didelės korporacijos, ta pati informacija galėtų būti panaudota apribojant individų galimybę susirasti darbą, gauti paskolą, apsidrausti ar nusipirkti būstą. Tikėtina, jog tobulėjant duomenų agregavimo technologijoms, vis daugiau verslų priims sprendimus vadovaudamiesi didžiųjų duomenų programų suformuotomis išvadomis[35]. Negana to, tikėtina, jog nuspėjamuosius modelius naudojantys verslo subjektai ar net valstybės, tokias praktikas laikys griežtai konfidencialiomis ir individai net neįtars, kas gali būti įrašyta jų „byloje“. Akivaizdu, jog agregavimo technologijų suformuoti spėjimai vis daugiau nulems asmenų gyvenimo galimybes,

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

[32] Žr. išnaša Nr. 9: Andrejevic ir Gates, „Big Data Surveillance,“ p. 190–91.

[33] 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.

[34] 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.

[35] Žr. išnaša Nr. 23: Hirsch, „That’s Unfair! Or Is It? Big Data, Discrimination and the FTC’s Unfairness Authority“, p. 345.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

todėl net ir menkiausia klaidinga algoritmo interpretacija galėtų turėti pragaištingų pasekmių žmogaus galimybei užsidirbti, susirasti darbą, keliauti, mokytis ir panašiai[36].

Agregavimas yra bevertis, jeigu nėra duomenų, kuriuos galima būtų analizuoti ir interpretuoti. Todėl, nors bepiločiai orlaiviai informacijos analizės ir interpretavimo procese praktiškai nedalyvauja, tačiau prie šio agregavimo pažeidimo prisideda įgalindami oportunistinį, visur esantį informacijos rinkimą. Tuo tarpu agregavimas, suporuotas su milžinišku kiekiu informacijos, gali būti labai pavojingas. Kaip jau buvo minėta, agregavimas sukuria neproporcingą galios pusiausvyrą visuomenėje, kur viską valdyti gali tie, kurie valdo informaciją. Net ir nepiktnaudžiaujant surinkta informacija, agregavimo programinės įrangos užfiksuotos elgesio struktūros ne visada gali atitikti tiesą, todėl gali sukelti nepagrįstus išankstinius nusistatymus, nulemsiančius žmonių gyvenimus. Tačiau net ir agregavimas nebūtų toks pavojingas, jeigu ne dar vienas pažeidimas, suteikiantis galimybę atpažinti stebimus individus. Toliau bus kalbama apie *Identifikavimą*.

## Identifikavimas

*Identifikavimas* yra tikrosios informacijos apie individą atskleidimas, kuris leidžia skaitmeninėse duomenų bazėse esančią informaciją pritaikyti konkrečiam asmeniui. Kitaip tariant, identifikavimas yra informacijos susiejimas su konkrečiais individais[37]. 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 panašiai.

Kita vertus, yra ir neigiama identifikavimo pusė. Tapatybės nustatymas individams užkrauna informacinį bagažą, kuris gali prieš juos sukelti išankstinį nusistatymą. Pavyzdžiui, Europos Žmogaus Teisių Teismo byloje Prancūzijos pilietis norėjo savo asmens dokumentuose (tapatybės kortelėje, pase ir balsavimo kortelėje) pasikeisti lytį, kadangi buvo chirurginiu būdu pasikeitęs lytį iš vyriškos į moterišką, tačiau Prancūzijos teisinė sistema tokios galimybės nenumatė. Kadangi asmens kode atsispindėjo asmens lytis ir kadangi šis kodas yra atskleidžiamas daugeliui institucijų, tai neleido asmeniui nei nuo potencialaus darbdavio, nei nuo darbdavio administracijos, nei nuo valstybės institucijų ar jų darbuotojų, nei nuo bankų paslėpti fakto, kad jis yra transseksualas. Teismo nuomone, apribojimas pasikeisti lytį asmens dokumentuose pažeidė asmens teisę į privatų gyvenimą[38]. Ši byla yra vienas iš akivaizdžių pavyzdžių, kada identifikavimas, pririšdamas individus prie praeities, nuo kurios jie gali norėti pabėgti, gali slopinti jų galimybę keistis ir trukdyti jų saviugdai[39].

Identifikavimas taip pat padidina valstybės galią individų atžvilgiu. Daugelyje valstybių biometriniai duomenys, tokie kaip asmens kodas, vardas, pavardė, žmonėms yra suteikiami vos gimus. Jų neturint būtų sudėtinga gyventi visuomenėje, nes identifikuoti save jau privaloma kone kiekviename gyvenimo žingsnyje – kai norime atsidaryti banko sąskaitą, kai prisijungiame prie elektroninės bankininkystės paskyros, kai atliekame notarinius sandorius, kai keliaujame į kitą valstybę. Surinktus duomenis valstybės gali panaudoti ne tik savo piliečių apsaugai, pinigų plovimo, terorizmo, nusikaltimų prevencijai, bet ir siekdamos apriboti žmonių judėjimą, slopinti

[36] Ten pat, p. 346.
[37] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 511.
[38] B vs France.pdf, No. 57/1990/248/319 (European Court of Human Rights 1992 m. sausio 24 d.).
[39] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 477.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

nepasitenkinimą valstybine santvarka, izoliuoti tam tikras visuomenės grupes. R. Sobel teigimu, identifikavimo sistemos turi ilgą naudojimo, piktnaudžiavimo socialine kontrole ir diskriminavimo istoriją. Pavyzdžiui, Sovietų Sąjungoje dirbančiajai klasei nebuvo išduodami pasai siekiant apriboti jų judėjimą. Dirbantieji, kurie turėjo pasus, galėjo gyventi ir kitose valstybės vietose, tačiau keliauti galėjo tiktai su milicijos, kuri kontroliavo žmonių judėjimą šalies viduje, leidimu ir tik į tam tikras vietas[40]. 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, pavyzdžiui, statutai, neleidžiantys komunistinių organizacijų nariams atnaujinti ar naudotis galiojančiu JAV pasu[41]. Prieš Antrąjį pasaulinį karą nacių Vokietijoje ir Antrajam pasauliniam karui prasidėjus jos okupuotose teritorijose tapatybės kortelės buvo naudojamos žydams izoliuoti ir surašyti. Kaip pastebi R. Sobel, visi su žydais susiję holokausto žiaurumai prasidėjo būtent nuo paprastų surašymų, t. y. nuo jų identifikavimo[42].

Identifikavimas taip pat neleidžia asmeniui išlaikyti anonimiškumo ar pseudonimiškumo. Anonimiškumas ar pseudonimiškumas leidžia žmonėms laisviau balsuoti, kalbėti, burtis į bendruomenes, kadangi apsaugo nuo išankstinio nusistatymo, šališkumo ar pavojaus, kad su jais bus susidorota. Anonimiškumas taip pat gali padidinti rašytojo idėjų įtikinamumą, nes skaitytojas, nežinodamas tikslaus autoriaus, gali lengviau priimti jo idėjas, nepaisydamas savo išankstinių nusistatymų. Dėl šios priežasties daugumoje universitetų egzaminai yra vertinami anonimiškai. Anonimiškumas taip pat suteikia galimybę žmonėms kritikuoti kontraversiškas įmonių, kuriose dirba, praktikas, ir be asmeninių pasekmių atskleisti apie jas kompromituojančius faktus[43]. Negana to, anonimiškumas gali apsaugoti žmones, kurie skaito ar klauso tam tikrų nepopuliarių idėjų[44].

Identifikavimas dažnai yra neatsiejamas kitų privatumo pažeidimų komponentas, todėl pažeidimų gali būti įvairių. Pavyzdžiui, vienu atveju, stebėseną vykdančiam subjektui gali užtekti užfiksuoti žmonių skaičių, judėjimo struktūras, lytį, apytikrį amžių, tačiau kitu atveju, kai norima sistemingai stebėti konkretų individą, gali reikėti identifikuoti stebimojo tapatybę. Identifikavimas taip pat gali būti agregavimo dalis. Agregavimu sukuriamas skaitmeninis statistinio žmogaus profilis, susidedantis iš tarpusavyje suderintų fragmentų, tačiau identifikavimas duomenų valdytojui suteikia galimybę žengti dar vienu žingsniu toliau – tą patį skaitmeninio žmogaus profilį galima tiesiogiai susieti su asmeniu realiame pasaulyje[45].

Naujausios technologijos, pagrinde veidų atpažinimo technologijos bei dronai, individų identifikavimo galimybes perkelia į naują lygmenį. Pavyzdžiui, Kinijos gatvėse jau veikia pažengusi sekimo sistema, kuri geba automatiškai nustatyti praeivių tapatybes. Nors Kinijos vyriausybė teigia, kad ši naujovė bus naudojama susekti pabėgėlius ir atrasti dingusius žmones,

[40] Richard Sobel, „The degradation of political identity under a national identification system“, *BUJ Sci. & Tech. L.* 8 (2002 m.), p. 52.

[41] Ten pat, p. 49.

[42] Ten pat, p. 50.

[43] 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.

[44] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 515.

[45] Ten pat, p. 477.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

tačiau ja akivaizdžiai galima bus piktnaudžiauti[46]. Maya Wang[47] teigimu, tokių sistemų tikslas yra suregzti tvirtesnį socialinės kontrolės tinklą, kuris apsunkintų žmonių galimybę planuoti veiksmus prieš vyriausybę arba spausti vyriausybę imtis reformų[48]. Vienintelis tokios sistemos apribojimas yra tai, kad stacionarios CCTV kameros, atpažinusios individo veidą, negali jo toliau sekti ten, kur stacionarių kamerų sistema neišvystyta arba tuo atveju, jeigu individas sistemingai vengia stacionarių stebėjimo sistemų, tačiau ir šią problemą galima išspręsti su dronais, kurių dėka jokių kliūčių toliau sekti stebimąjį nebelieka.

Dronais surinkti ir duomenų bazėse patalpinti vaizdiniai duomenys, kuriuose individų tapatybės nenustatytos, yra tik skaitmeninės beveidžių žmonių gyvenimo nuotrupos, todėl tokiu plačiu privatumo pažeidimo mastu nepasižymi. Tačiau, kai dronai realiu laiku sugebės atpažinti stebimąjį, individai galės būti susiejami su didelėmis duomenų bazėmis visur ir visada to net nežinodami ir nedavę tam sutikimo. Nesunkiai galima įsivaizduoti scenarijų, kai iš kalinimo įstaigos pabėga kalinys ir valstybės institucija savo paieškos sistemoje įveda šio individo asmens kodą ir paskelbia jo paiešką. Tiesiog mygtuko paspaudimu pabėgėlio duomenys žaibiškai perduodami milijonams stacionarių vaizdo kamerų, kad šios ieškotų norimo asmens veido. Vos tik stacionari kamera atpažįsta pakankamai tikėtiną atitikmenį, sistema automatiškai iš artimiausios stoties paleidžia kameromis ir tokiais pat veido atpažinimo algoritmais apginkluotus dronus. Po kelių minučių individą iš visų pusių apsupa trys autonomiškai veikiantys dronai, kurie akimirksniu tiksliai identifikuoja stebimą subjektą, nustato, ar jis nepavojingas visuomenei. Nustatyti duomenys tuojau pat perduodami operatyviniam policijos būriui, kuris, priklausomai nuo pabėgėlio pavojingumo lygio, imasi atitinkamo lygio sulaikymo veiksmų. Vieno eksperimento metu, kuriuo buvo siekiama parodyti veido atpažinimo technologijos galimybes, Kinijos valdžia, naudodamasi savo stacionarių CCTV kamerų sistema su veido atpažinimo algoritmais, sugebėjo BBC žurnalistą surasti ir sulaikyti vos per 7 minutes[49].

Taigi Identifikavimo pažeidimas yra tiesiogiai susijęs su bepiločiais orlaiviais, kuriuos labai nesunku įsivaizduoti naudojant veido atpažinimo programinę įrangą, turint mintyje, jog beveik kiekvienas jų turi vaizdo kamerą. Būtent identifikavimas suteikia galimybę filmuotoje medžiagoje esantį žmogų susieti su konkrečiu profiliu ir vėliau šią informaciją panaudoti prieš atpažintą asmenį.

## Saugumo neužtikrinimas

Duomenys yra žinios, žinios yra galia, o galia visada virsta į pinigus. Internetinė parduotuvė, rinkdama duomenis apie savo lankytojų elgesį, gali lengviau nuspėti, ką klientai gali norėti pirkti. Kai pirkėjo pomėgiai aiškūs, įtikinti jį ką nors įsigyti tampa žymiai paprasčiau, pavyzdžiui, rekomenduojant jam įsigyti įvairias prekes vietoje to, kad pirkėjas pats į paiešką įvestų norimą prekę. Individas net nepajunta, kaip duomenys apie jo įsigytas prekes, pristatymo adresą, palikti atsiliepimai prie nupirktų prekių, išverčiami į stebėtinai tikslius pardavėjo spėjimus

[46] „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/.

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

[48] Žr. išnaša Nr. 46: „In China, Facial Recognition Tech Is Watching You.“

[49] „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/.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

apie asmens pomėgius, turtinę padėtį ir prekes, kurias jis gali norėti įsigyti. Tokiu būdu duomenys tampa pinigais. Puikus pavyzdys yra Amazon, kuri pradėjo kaip internetinė knygų parduotuvė, tačiau rinkdama duomenis apie lankytojų elgesį savo tinklapyje ir šiuos duomenis analizuodama, sugebėjo tapti viena daugiausiai uždirbančių bendrovių pasaulyje.

Kadangi informacija šiais laikais yra tokia vertinga, tiek ją parduodančių programišių, tiek norinčių ją įsigyti kompanijų juodojoje rinkoje tikriausiai netrūksta, nes kibernetinių atakų skaičius kiekvienais metais tiktai auga.[50] Rinkoje šiais laikais apskritai sunku būtų rasti nors vieną internetine rinkodara pasikliaujantį gigantą, iš kurio nebūtų pavogti milijonų žmonių asmens duomenys. Nors duomenų bazės su jautria informacija apie žmonių elgesį, slaptažodžius, banko kortelių duomenis turėtų būti patikimai saugomos, tačiau aibė milžiniškų kibernetinio saugumo skandalų, tarp jų Yahoo[51], Marriott International[52], Ebay[53], parodo, kad įsilaužti įmanoma bet kur.

Daugelis duomenų apsaugos teisės aktų numato, kad asmens duomenys privalo būti tvarkomi tokiu būdu, kad užtikrintų pakankamą saugumo lygį. Pavyzdžiui, BDAR 5 straipsnio 1 dalies f punktas numato, kad „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)“[54]. JAV 1974 Privatumo Aktas reikalauja, kad federalinės agentūros, kurios tvarko asmens duomenis, įtvirtintų tinkamas administracines, technines ir fizines apsaugos priemones, kad būtų užtikrintas įrašų saugumas ir konfidencialumas[55]. Vis dėlto vien teisės aktuose įtvirtinta duomenų valdytojų pareiga užtikrinti asmens duomenų saugumą savaime nėra pakankama. Kibernetinių vagysčių gausa dvidešimt pirmajame amžiuje rodo, kad duomenų gavybos gigantai

[50] Pavyzdžiui, vien JAV nuo 2006 iki 2015 metų kibernetinių atakų padaugėjo 1300 procentų, 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.

[51] 2016 m. rugsėjo mėn. Yahoo paskelbė, kad kibernetinės atakos metu iš Yahoo duomenų saugyklų buvo pavogti apie 3 milijardų 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.

[52] 2018 m. lapkričio mėn. Marriott International paskelbė, kad kibernetiniai vagys pavogė apie 500 milijonų 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., posk. U.S., https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[53] Internetinių pirkimų gigantas Ebay 2014 m. paskelbė, kad per kibernetinę ataką buvo pavogti 145 milijonų 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/.

[54] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“ (Bendrasis duomenų apsaugos reglamentas), OJ L 119, 2016-05-04, p. 1–88 (LT).

[55] The Privacy Act of 1974, pakeistas 5 U.S.C. § 552a.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

yra labiau pajėgūs informaciją kaupti ir analizuoti, negu ją apsaugoti. Duomenų valdytojų negebėjimas apsaugoti sukauptų duomenų vadinamas *saugumo neužtikrinimu*[56].

Dronai su šiuo privatumo pažeidimu gali būti susiję trejopai. Viena, dronai įgalina rinkti tokią informaciją apie individus, kuri anksčiau buvo neprieinama, todėl dronų technologija išplečia duomenų, kurie gali būti pavogti iš netinkamai apsaugotų duomenų bazių, apimtį. Pavyzdžiui, pristatydamas siuntinį į namus, dronas gali užfiksuoti realų asmenį, kuris užsisakė tam tikrą prekę, gali nufilmuoti jo namų apylinkes, buitį, gali užfiksuoti duomenis, kurie sklinda bevieliu ryšiu, kryptiniu mikrofonu pasiklausyti namų gyventojų pokalbių, kitų namuose sklindančių garsų. Dronai nėra pirmoji technologija, kuri įgalina kaupti duomenis apie individų elgesį realiame pasaulyje, juk kone kiekvienas naudojamės išmaniaisiais telefonais, kurie turi mikrofonus ir filmavimo kameras, kai kurie jau naudojasi išmaniaisiais namų asistentais, tokiais kaip Amazon Echo Dot ar Google Home, kurie turi galingus mikrofonus. Teoriškai labai didelę dalį informacijos apie žmogaus elgesį realiame gyvenime galima kaupti pasitelkiant vien šiuos įrenginius. Tačiau kaip ir minėtos technologijos, dronai prie saugumo neužtikrinimo prisideda tuo, kad įgalina didelę galią rinkoje turinčius subjektus dar vienu būdu išgauti duomenis apie asmenų elgesio struktūras ir galiausiai dar didesnės apimties sukauptų duomenų negebėti apsaugoti nuo kibernetinių atakų.

Antra, kibernetiniai užpuolikai gali įsilaužti ne tik į duomenų bazes, kuriose kaupiami dronais surinkti duomenys, bet ir į pačius dronus individualiai. Drono veikimas yra visiškai priklausomas nuo bevielio duomenų ryšio, kuris sieja skirtingus drono komponentus tarpusavyje. Kiekvienas dronas turi skirtingas ryšių sąsajas, kurioms apsaugoti yra naudojamos skirtingos apsaugos priemonės, pavyzdžiui, skraidančioji drono dalis beveik visais atvejais bevieliu 4G ar Wi-Fi ryšiu būna susieta su valdymo stotimi, taip pat GPS / Galileo ryšiu su palydovu žemės atmosferoje, autonominiai dronai gali papildomai būti susieti tarpusavyje, kad sudarytų kolektyvinį spiečių. Mokslinėje literatūroje pripažįstama, kad satelitinį ir tiesioginį duomenų ryšį (kai dronas valdomas tiesiogiai iš neprijungtos prie interneto valdymo stoties) nulaužti sudėtingiau, nes šiems ryšiams apsaugoti egzistuoja pakankamai patikimos apsaugos priemonės[57], o į Wi-Fi tinklus įsibrauti įmanoma gana lengvai, nes jiems apsaugoti naudojami metodai yra nesaugūs ir nepatikimi[58]. Nulaužus individualų droną, programišiai gali perimti jo valdymą, slapta stebėti ir pasiklausyti aplinkos per drono vaizdo kameras ir mikrofonus, nustatyti asmenų buvimo vietą[59]. Nors įsilaužimas į atsitiktinio individualaus drono sistemą gali atrodyti savaime nelabai pavojingas, kadangi, galima pamanyti, pažeidžiamas tiktai individualaus drono valdytojo privatumas, tačiau problema slypi giliau. Įsilaužimas į individualaus drono sistemą tinkamoje vietoje ir tinkamu laiku gali sukelti grėsmę daugelio kitų žmonių privatumui, kadangi nulaužtas dronas gali būti panaudojamas piktadarystėms ne tik prieš drono valdytoją, bet ir prieš kitus individus.

[56] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 516–522.

[57] 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.

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

[59] 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.), p. 15, https://doi.org/10.1117/12.902990.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

Iš to kyla trečiasis saugumo neužtikrinimo aspektas – patys dronai gali būti priemonės kibernetiniams išpuoliams vykdyti. Pavyzdžiui, dronai gali būti naudojami nusikaltimo vietų modifikavimui. Pasitelkdami bepiločius orlaivius, nusikaltėliai galėtų iš įvykio vietos pašalinti savo nusikaltimo pėdsakus arba pridėti padirbtų pėdsakų bei tokiu būdu sudaryti pagrindą klaidingiems kaltinimams. Pirštų antspaudus jau dabar įmanoma padirbti specialiu spausdintuvu, šią technologiją tiesiog reikėtų pritaikyti dronams[60]. Dar vienas pavyzdys galėtų būti naujos kartos botų tinklai. Mokslininkų grupė neseniai pristatė droną, kuriuo galima automatiškai aptikti ir įsilaužti į Wi-Fi tinklus. Savo straipsnyje Theodore Reed, Joseph Geis ir Sven Dietrich pristato plačiai naudojamą įsilaužimo į vietinius Wi-Fi tinklus sistemą – *botų tinklą*[61], kuri, autorių teigimu, šiuo metu yra didžiausia grėsmė kibernetiniam saugumui ir pristato savo botų tinklo variantą – SkyNET, kuriuo galima įsilaužti į asmenų kompiuterius ne internetu, o pasitelkiant droną, kuris nulaužia vietinius Wi-Fi tinklus iš oro. Įprastą *botų tinklą* internetu kontroliuoja *botmasteris*[62], tačiau tokiu būdu veikiantys botų tinklai pasitelkiant šiuolaikines kibernetinio saugumo priemones jau gali būti susekami, tuo tarpu SkyNET dronai gali būti kontroliuojami be interneto pagalbos, todėl apeina tokias tradicines internetinių tinklų apsaugos priemones kaip ugniasienės (angl. firewalls), įsilaužimo aptikimo sistemos (angl. intrusion detection systems) ir įvykių registravimas (angl. event logging). Negana to, asmeninių Wi-Fi tinklų apsauga paprastai būna labai silpna, todėl per juos įsilaužti į šeimininko kompiuterį visai nesudėtinga[63]. Taigi SkyNET įgalina programišius lengvai įsilaužti į žmonių kompiuterius tiesiog dronu praskrendant pro juos dominančią vietovę[64], belieka tik įsivaizduoti, kokio masto kibernetiniai nusikaltimai galėtų būti įvykdyti, jeigu į darbą būtų paleistas ne vienas, o šimtai ar tūkstančiai SkyNET principu veikiančių dronų.

Kaip matyti iš atliktos analizės, dronai prie saugumo neužtikrinimo privatumo pažeidimo prisideda labai reikšmingai ne tik dėl to, kad padidina surinktą informacijos kiekį nesaugiose duomenų bazėse, bet ir dėl to, kad patys įgalina programišius vykdyti kibernetinius nusikaltimus, kurie dar visai neseniai buvo mokslinės fantastikos sritis.

## Atidengimas

*Atidengimas* yra toks privatumo pažeidimas, kuriuo atkleidžiami tam tikri fiziniai ar emociniai individo atributai tretiesiems asmenims. Šiuos atributus žmonės paprastai vertina kaip giliai pirmykščius ir jų atskleidimas dažnai sukelia sumišimo arba pažeminimo jausmus. Prie šių atributų priskiriamas sielvartą, kančią, traumą, sužeidimus, nuogumą, lytinius santykius, šlapinimąsi ir tuštinimąsi – visi jie yra pirminiai žmonių gyvenimo aspektai, kurie yra fiziniai,

[60] Ten pat.

[61] Terminas „botnet“ į lietuvių kalbą galėtų būti verčiamas kaip „botų tinklas“, o terminas „botas“ pagal „Cambridge Dictionary“ suprantamas kaip „kompiuterinė programa, kuri veikia autonomiškai, ypatingai tokia, kuri ieško ir randa informaciją internete: nusikaltėliai sukuria botų tinklus, kurie klajoja internete užkrėsdami personalinius kompiuterius kenkėjiškomis programomis“ (autoriaus vertimas). „BOT | Meaning in the Cambridge English Dictionary“, žiūrėta 2019 m. gegužės 7 d., https://dictionary.cambridge.org/dictionary/english/bot.

[62] Terminas „botmaster“ į lietuvių kalbą galėtų būti verčiamas kaip „botmasteris“. Šis terminas išreiškia asmenį arba programą, kuri kontroliuoja botų tinkle esančius pavienius botus.

[63] Žr. išnaša Nr. 58: Reed, Geis, ir Dietrich, „SkyNET: A 3G-Enabled Mobile Attack Drone and Stealth Botmaster,“ p. 1–2.

[64] Ten pat, p. 3.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

instinktyvūs ir būtini. Vis dėlto šių laikų visuomenėje yra priimta manyti, jog šie natūralūs procesai atskleidžia individo silpnybes, padaro jį pažeidžiamą, kai kurios veiklos yra laikomos gyvuliškomis, pasibjaurėtinomis, todėl didžioji dauguma individų nenori atskleisti jų tretiesiems asmenims[65].

Suvokimas apie viešai demonstruojamą kūną ir jo funkcijas istorijos eigoje nebuvo vienodas[66]. Pavyzdžiui, viduramžiais žmonėms buvo įprasta nuogiems praustis kartu su nepažįstamaisiais, tačiau nuo šešiolikto amžiaus nuogą kūną buvo įprasta slėpti nuo kitų. Antikinėje Graikijoje viešas nuogumas buvo laikomas stiprybės ženklu, tuo tarpu renesanso laikotarpiu turtingieji jau drovėjosi savo kūnu ir jo funkcijomis[67]. Šių laikų socialinės normos reikalauja kai kurias kūno dalis ir funkcijas laikyti slaptomis, todėl jų *atidengimas* visuomenei be individo sutikimo yra laikomas žmogaus orumo, todėl ir privatumo pažeidimu. Kaip teigia D. Solove, orumas šiuolaikiniu suvokimu suteikia galimybę individui peržengti savo žvėrišką prigimtį ir tokiu būdu tapti civilizuotu[68].

Dauguma žmonių, pamatę kitą asmenį nuogą, užsiimantį lytiniais santykiais ar atliekantį gamtinius reikalus, tikriausiai nemanytų, jog jis už juos menkesnis ar mažiau civilizuotas, juk visi tuos pačius dalykus kiekvieną dieną atlieka ir jokių naujienų tame nėra, tačiau pažeidimo auka, be kurios sutikimo tokios veiklos yra atidengiamos tretiesiems asmenims, prieš kitus gali jaustis menkesnės ir mažiau civilizuotos. Individas vien žinodamas, kad tokia informacija apie jį ar ją yra surinkta, gali sukelti jam nesaugumo jausmą, paranoją. Viešai paskelbta tokio pobūdžio informacija asmeniui gali sukelti pažeminimą, kuris gali pažeisti jo pasitikėjimą savimi, savivertę. Visuomenė *atidengimo* pažeidimo aukų paprastai nesmerkia dėl jų veiksmų, kadangi atskleista tokio pobūdžio informacija visiems nėra naujiena, tačiau tokio pažeidimo aukos psichologiškai nukentėti gali labai stipriai[69].

Dronai prie šio privatumo pažeidimo prisideda dėl to, kad jais žmones nufilmuoti ar nufotografuoti privačioje erdvėje užsiimant privačiais reikalais yra lengviau nei kada nors anksčiau. Užfiksuotų dronų vojerizmo atvejų netrūksta. Pavyzdžiui, JAV Kentukio valstijoje vyras šautuvu numušė virš savo žemės sklypo pakibusį droną neva dėl to, kad dronu buvo stebima kieme besideginanti šešiolikmetė dukra[70]. Pora iš Bremeno Vokietijos policijai pateikė pranešimą apie pro miegamojo langą juos stebintį droną[71]. Kita pora iš Regestauf, Vokietijos, taip pat policijai teigė, kad kažkas dronu juos stebėjo per svetainės langus[72]. Moteris iš Atlantos, JAV,

[65] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 536.
[66] Ten pat, p. 537.
[67] Daniel J. Solove, „Conceptualizing privacy“, *Calif. L. Rev.* 90 (2002 m.), p. 1087-1156.
[68] Žr. išnaša Nr. 6: Solove, „A Taxonomy of Privacy,“ p. 537.
[69] Ten pat, p. 538.
[70] 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/.
[71] 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.
[72] 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.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

skundėsi, jog per dangoraižyje esančio buto langus dronu kažkas stebėjo, kaip ji rengiasi[73]. Visais paminėtais atvejais išpuolių aukas kompromituojanti vaizdinė medžiaga viešai atskleista nebuvo, tačiau vien tikimybė, kad asmuo bet kuriuo metu gali būti stebimas per namų langus, sukelia jam tam tikrą psichologinį spaudimą, kuris gali būti traktuojamas kaip privatumo pažeidimas. Individas, žinodamas, kad net ir būdamas visiškai vienas savo namų aplinkoje, gali būti stebimas, jaučia pastovią įtampą ir nesaugumą, o tai jau sukelia moralinę žalą. Dar didesnė psichologinė žala kyla tuomet, kai užfiksuota vaizdinė medžiaga būna atskleidžiama viešai. Labiausiai tikėtini atskleidimo scenarijai galėtų būti susiję su viešomis figūromis[74], tačiau nesunku įsivaizduoti ir atvejų, kada kompromituojantys vaizdo įrašai ar nuotraukos galėtų būti panaudojami šantažui[75].

Taigi anksčiau retas asmuo, būdamas savo namų erdvėje, būtų pagalvojęs, kad kažkas jį/ją stebi per langus ar uždarame kieme, tačiau atsiradus dronams situacija iš esmės keičiasi. Dabar net ir gyvenantys dangoraižiuose prieš persirengdami savo namuose pagalvos, ar nereikėtų prieš tai užtraukti užuolaidas, o norintys pasideginti uždarame savo namų kieme pagalvos, ar nori apsinuoginę pasirodyti neapibrėžtam asmenų ratui, jeigu kartais pro jų kiemą praskristų kaimyno valdomas bepilotis. Dronai, kaip ir daugelio kitų privatumo sutrikdymo atveju, yra tik informacijos rinkimo priemonė, tačiau be jos daugeliu atvejų *atidengimo* pažeidimas negalėtų būti įvykdomas visiškai arba būtų įvykdomas žymiai rečiau.

# IŠVADOS

1. Per privatumo pažeidimų prizmę atlikta analizė parodė, kad bepiločiai orlaiviai yra rimta grėsmė privatumui. Šiame straipsnyje aptartais būdais privatumą pažeisti įmanoma buvo ir anksčiau, tačiau dronų dėka, jų dažnumas ir sunkumas gali ženkliai išaugti. Iš atliktos analizės galima išskirti kelias pagrindines priežastis, kodėl bepiločiams orlaiviams gali reikėti specialaus privatumo reguliavimo:
    - **Platus naudojimo mastas.** Lanksčios bepiločių orlaivių pritaikymo galimybės, taip pat maža kaina, nedideli gabaritai lems tai, jog netolimoje ateityje danguje jų bus labai dideli kiekiai. Daug asmens duomenis galinčių fiksuoti robotų danguje reiškia neribotas galimybes galingiems informacijos infrastruktūrą valdantiems viešiems ir privatiems subjektams užfiksuotą informaciją panaudoti saviems tikslams pasiekti.
    - **Stebėjimo intensyvumas.** Dronais žmones įmanoma stebėti nuolatos ir iš labai arti, o užfiksuotus vaizdus talpinti laikmenose, kur jie vėliau gali būti

[73] 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.

[74] „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.

[75] Pavyzdžiui, vieną šantažo atvejų puikiai perteikia mokslinės fantastikos serialo „Juodasis veidrodis“ (angl. Black Mirror) serija „Užsičiaupk ir šok“ (angl. Shut Up and Dance), kurioje pagrindinis veikėjo devyniolikmečio kompiuteris užkrečiamas virusu. Jam nežinant kenkėjiška programa aktyvuoja nešiojamo 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).

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

iš naujo atrasti ir perdirbti. Iki atsirandant UAS, intensyviausio stebėjimo sistema buvo CCTV stebėjimo kameros, kurios privalo būti pritaisytos prie stacionarių objektų, dėl to jų patikimumas detaliai atkurti įvykius ar žmones ribotas.

- **Stebėjimo kampų įvairovė.** Dronai gali įveikti kliūtis, esančias jų matymo linijoje ir dėl skraidymo galimybių užfiksuoti tokius vaizdus, kurių prie nejundačio objekto pritaisyta kamera užfiksuoti negalėtų. Naudojant specialią programinę įrangą bepiločiu orlaiviu ar jų spiečiumi galima užfiksuoti netgi trimatį stebimo objekto vaizdą, ko negalėtų pasiūlyti iki dronų atsiradimo naudotos stebėjimo priemonės. Nuolatinę stebėseną bepiločiais orlaiviais galima vykdyti ne tik viešose vietose, kur ir taip daug stacionarių stebėjimo kamerų, bet ir, pavyzdžiui, prie stebimojo durų slenksčio.
- **Galimybė tapti ginklu.** Dronai gali būti apginkluoti ne tik kamera, bet ir siųstuvais, kurie gali padėti atlikti kibernetinę ataką, garsiakalbiais, kuriais gali būti bandoma įbauginti taikų asmenų susibūrimą, ar 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. Dronus paversti skraidančiais, visa matančiais ginklais, kuriais be reikšmingų apribojimų naudojasi valstybės apsaugos tarnybos, užtektų neapgalvoto valdžios institucijų sprendimo, pavyzdžiui, kriziniu laikotarpiu, todėl bepiločiai orlaiviai šiuo aspektu pavojingiausi biurokratų rankose.
- **Paslaptingumas.** Bepiločiai orlaiviai gali būti įvairių konfigūracijų. Kai kurie būna dideli ir skleidžia daug garso, juos lengva pastebėti. Vis dėlto, tikėtina, jog stebėsenai pritaikyti dronai įgys įvairių „nematomų“ formų, pavyzdžiui, Kinija jau dabar kuria dronus, kurie panašūs į balandžius. Ateityje sekimui naudojami UAS tikriausiai primins vos įžiūrimus vabzdžius. Tokių bepiločių orlaivių paslaptingumas gali lemti tai, kad stebimi individai nežinos nei kokiu pagrindu yra sekami, nei kad yra sekami apskritai, nei kokius su jais susijusius sprendimus vadovaudamiesi surinkta informacija priims duomenis kaupiantys subjektai.

2. Taigi dronų technologija dėl išskirtinių savybių, kuriomis nepasižymi nei viena iki šiol prieinama stebėsenos priemonė, sukuria puikią infrastruktūrą oportunistiniam informacijos rinkimui realiame pasaulyje. Kaip parodė atlikta analizė, tinkamai nereglamentuotas jų naudojimas gali paveikti individų psichologiją, socialinių grupių ir skirtingų visuomenės sluoksnių elgseną bei demokratinės santvarkos stabilumą. Todėl labai svarbu, kad dronų naudojimas būtų reguliuojamas atsižvelgiant ne tik į grėsmę žmonių sveikatai / gyvybei, bet ir realius pavojus privatumui.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

# ŠALTINIŲ SĄRAŠAS

## Teisės aktai

1. „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“ (Bendrasis duomenų apsaugos reglamentas), OJ L 119, 2016-05-04, p. 1–88 (LT).
2. „2019 m. gegužės 24 d. Komisijos įgyvendinimo reglamentas (ES) 2019/947 dėl bepiločių orlaivių naudojimo taisyklių ir tvarkos“, OL L 152, 2019-06-11, p. 45—71.
3. Lietuvos Respublikos Civilinio proceso kodeksas (suvestinė redakcija nuo 2020-07-09), *Žin.* (2002-04-06, Nr. 36-1340 ).
4. Lietuvos Respublikos elektroninių ryšių įstatymas (suvestinė redakcija nuo 2020-01-17) (Žin., 2004, Nr. 69-2382).
5. The Privacy Act of 1974, pakeistas 5 U.S.C. § 552a.

## Teismų praktika

6. B vs France.pdf, No. 57/1990/248/319 (European Court of Human Rights 1992 m. sausio 24 d.).

## Kiti šaltiniai

7. „BOT | Meaning in the Cambridge English Dictionary“, žiūrėta 2019 m. gegužės 7 d., https://dictionary.cambridge.org/dictionary/english/bot.
8. „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/.
9. „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.
10. „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/.
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.

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

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 ., http://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/.
15. „Watergate Scandal | Summary, Timeline, & Deep Throat“, Encyclopedia Britannica, žiūrėta 2020 m. rugpjūčio 27 d., https://www.britannica.com/event/Watergate-Scandal.
16. „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.
17. Andrejevic, Mark ir Kelly Gates, „Big Data Surveillance: Introduction“, *Surveillance & Society* 12, Nr. 2 (2014 m. gegužės 9 d.), p. 185–96, https://doi.org/10.24908/ss.v12i2.5242.
18. Bentham, Jeremy, *Panopticon Or the Inspection House* (T. Payne, 1791).
19. Bonetto, Margherita ir kt., „Privacy in mini-drone based video surveillance“, *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, t. 4 (IEEE, 2015 m.), p. 1–6.
20. Calo, Ryan M., „The Drone as a Privacy Catalyst“, *Stanford Law Review Online* 64 (2011 m.), p. 29–33; Rocci Luppicini ir Arthur So, „A technoethical review of commercial drone use in the context of governance, ethics, and privacy“, *Technology in Society* 46 (2016 m. rugpjūčio 1 d.), p. 109–19, https://doi.org/10.1016/j.techsoc.2016.03.003.
21. Choi, Sophia, „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.
22. Clarke, Roger, „The regulation of civilian drones’ impacts on behavioural privacy“, *Computer Law & Security Review* 30, Nr. 3 (2014 m. birželio 1 d.), p. 286–305, https://doi.org/10.1016/j.clsr.2014.03.005.
23. Clarke, Roger, Introduction to dataveillance and information privacy (Australian National University, 2006).
24. Esteban, Cristina Fernández, „China is testing creepy drones that look and fly like real birds to monitor citizens“, Business Insider, žiūrėta 2020 m. rugpjūčio 24 d., https://www.businessinsider.com/china-is-testing-creepy-dove-drones-to-monitor-citizens-2018-6.
25. Feigenbaum, Joan ir Bryan Ford, „Seeking Anonymity in an Internet Panopticon“, *Commun. ACM* 58, Nr. 10 (2015 m.), p. 58–69, https://doi.org/10.1145/2714561.
26. Finn, Rachel L. ir David Wright, „Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications“, *Computer Law & Security Review* 28, Nr. 2 (2012 m. balandžio 1 d.), p. 184–94, https://doi.org/10.1016/j.clsr.2012.01.005.
27. Finn, Rachel L., David Wright, ir Michael Friedewald, „Seven types of privacy“, European data protection: coming of age (Springer, 2013).

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

28. Haggerty, Kevin D., Richard V. Ericson, „The Surveillant Assemblage“, *British Journal of Sociology* 51, Nr. 4 (2000 m. gruodžio 1 d.), p. 606, https://doi.org/10.1080/00071310020015280.
29. Hirsch, Dennis D, „That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority“, *Kentucky Law Journal* 103 (2014 m.), p. 350.
30. Javaid, Ahmad 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.
31. Kasper, Debbie V. S. „The evolution (or devolution) of privacy“, Sociological Forum, t. 20 (Springer, 2005), 69–92.
32. Kitchin, Rob, „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.
33. Matyszczyk, Chris, „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/.
34. McBride, Paul, „Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations Comment“, *Journal of Air Law and Commerce* 74 (2009 m.), p. 627–62.
35. 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.
36. 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.
37. Norgall, Von Sabine „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.
38. Orwell, George ir A. M. Heath, *Animal farm and 1984* (Houghton Mifflin Harcourt, 2003).
39. Packer, Jeremy, „“Epistemology Not Ideology OR Why We Need New Germans”“, *Communication and Critical/Cultural Studies* 10, nr. 2–3 (2013 m. rugsėjo mėn.), p. 298, https://doi.org/10.1080/14791420.2013.806154.
40. Popken, Ben, „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.
41. Pūraitė, Aurelija, Daiva Bereikienė, ir Neringa Šilinskė, „Regulation of unmanned aerial systems and related privacy issues in Lithuania“, *Baltic Journal of Law & Politics 10*, nr. 2 (2017 m.): 107–32.
42. Reed, Theodore, Joseph Geis, ir Sven Dietrich, „SkyNET: A 3G-Enabled Mobile Attack Drone and Stealth Botmaster.“, *WOOT*, 2011, p. 28–36.
43. Rieland, Randy, „Teaching Drones to Sniff Out Toxic Air“, Smithsonian Magazine, žiūrėta 2020 m. rugpjūčio 27 d.,

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

https://www.smithsonianmag.com/innovation/teaching-drones-sniff-out-toxic-air-180970231/.
44. Samland, Fred 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.), p. 15, https://doi.org/10.1117/12.902990.
45. Sanger, David E. 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., posk. U.S., https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.
46. Sobel, Richard, „The degradation of political identity under a national identification system“, *BUJ Sci. & Tech. L.* 8 (2002 m.), p. 52.
47. Solove, Daniel J., „A Taxonomy of Privacy“, *University of Pennsylvania Law Review* 154 (2005 m.), p. 477–564.
48. Solove, Daniel J., „I’ve Got Nothing to Hide and Other Misunderstandings of Privacy 2007 Editor’s Symposium“, *San Diego Law Review* 44 (2007 m.), p. 745-772.
49. Volovelsky, Uri, „Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study“, *Computer Law & Security Review* 30, Nr. 3 (2014 m. birželio 1 d.), p. 306–20, https://doi.org/10.1016/j.clsr.2014.03.008.
50. Watkins, James, *Shut Up and Dance*, Drama, Sci-Fi, Thriller (House Of Tomorrow, 2016).
51. West, Jonathan P. ir James S. Bowman, „The domestic use of drones: An ethical analysis of surveillance issues“, *Public Administration Review* 76, Nr. 4 (2016 m.), p. 649–659.

## SUMMARY

## DRONE THREATS TO PRIVACY: POSSIBLE INFRINGEMENTS

*The purpose of this article is to reveal what privacy breaches may result from the use of small drones (also known as drones or UAS). Many researchers studying the relationship between drone use and privacy acknowledge that UAS pose a threat to privacy, but in reaching such a conclusion, authors simply presume the impendence on the basis of one or few examples and do not discuss in detail specific privacy violations that can be caused by drone use. The article, based on Daniel Solove’s taxonomy of privacy violations, shows that the use of drones violates privacy in all ways. UASs are information gathering tools that can come in a variety of sizes and configurations; they can record both video and sound, capture thermal changes in the environment, detect chemical traces, capture wireless data traffic. Both public and private actors may want to use this technology to create a systematic and large-scale monitoring infrastructure that can have a cooling effect on society in the long run. However, combining drones with huge databases and aggregation software can lead to very unequal distribution of power in society; data may be prone to misuse by powerful entities, who may misinterpret individual behavior using*

ISSN 2029-4239 (online)
*Teisės apžvalga*
*Law review*
*No. 1 (23), 2021, p. 64-87*

*biased algorithms and create wrongfully founded prejudices. Unmanned aerial vehicles can be combined with facial recognition software that will allow real people to be associated with their profiles in cyberspace, which may contribute to constant surveillance not only on the internet, but also in the real world. Furthermore, there are concerns about the security of the data collected, the vulnerability of UASs to cyber-attacks, and their use as tools to conduct cyber-attacks. In addition to systemic problems, the ability of drones to be assigned to any individual at any angle provides opportunities for more frequent voyeur attacks. The article concludes that drones are a serious threat to privacy and outlines the main reasons why current regulation may not be sufficient to avoid the threats associated with drone use.*

## KEY WORDS

*Drones, UAS, privacy, violations, infringements, classification, taxonomy*.