Turiba University

Neringa Šilinskė

SYNOPSYS OF THE DOCTORAL THESIS

PRIVACY PROTECTION IN NATIONAL LEGISLATION RELATED TO THE USE OF VISUAL INFORMATION RECORDING DEVICES

Study programme: Civil Law

Elaborated for an award of doctoral degree
in Law Science
sub-branch: Civil Law

Riga, 2021

The doctoral was developed at the Law Faculty of Turiba University during the period 2015 to 2021.
Advisor:

Professor Dr. iur.: ***Aurelija Pūraitė***

Doctoral consultant:

Dr. iur: ***Ingrīda Veikša***

Official reviewers:

Dr. iur: ***Janis Grasis, BA School of Business and Finance, Assoc. Professor***
Dr. iur: ***Alvydas Šakočius, Military Academy of General Jonas Žemaitis, Professor***
Dr. iur: ***Violeta Vasiliauskienė, Mykolas Romeris University, Professor***

The defence/presentation of the doctoral thesis shall be held at the public sitting of the doctoral council of Turiba University for the Law science at **12:00, on the 6'th of October 2021** at the Faculty of Law, Turiba University, Graudu street 68, Riga, Room No. C108.

The doctoral thesis and synopsis can be reviewed at the library of Turiba University, Graudu street 68, Riga.

Chairperson of the doctoral council for _____ sciences:

Dr.iur.: ***Jānis Načisčionis***

Secretary of the doctoral council for _____ sciences:

Dr. iur.: ***Ingrīda Veikša***

Description of the problem. As the world changes rapidly, sometimes legal instruments do not go along with the challenges that these rapid changes have posed to the legal system. If happens so, people may start feeling insecure. In order not to lose people's faith in the efficiency of law and assure its reflection of current social processes, laws have to be reviewed and adjusted to relevant time and its achievements, so that these achievements and social processes are not suppressed in order to fit the existing laws which do not match the reality anymore.[1] It is important because the law cannot be fixed, as the world itself is not stable, and not only technological achievements are changing (such change is advantageous and should not be suppressed, otherwise it would stop the progress of society), but people's understating of various values is changing too. For example, who could a half-century ago have thought that the right to respect for private life would be escalated in the contexts such as the use of a work computer for personal (illegal) purposes,[2] disclosure of *CCTV* (closed-circuit television) footage,[3] or surveillance via GPS?[4]

Along with the development of modern technologies, we notice how it is becoming easy to gather and transfer information: with the help of drones we can capture images, record, conduct search; video recording, surveillance cameras mounted on buildings, in cars can capture visual information about everything that is on the way. The biggest amount and the most accurate information about private life is conveyed by visual data (photos or videos). The importance of an image has been described by the European Court of Human Rights (hereinafter – *ECHR*/the Court) which in one of its decisions has stated that "[A] person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development",[5] "the publication of a photograph must, in the Court's view, in general, be considered a more substantial interference with the right to respect for private life than the mere communication of the person's name".[6] Such importance of an image is affirmed by national courts.[7]

---

[1] Socio-legal positivism theory accepts the Social Fact Thesis which asserts that the content of law is manufactured according to social processes (Himma, K. E. (2004). Do Philosophy and Sociology Mix? A Non-Essentialist Socio-Legal Positivist Analysis of the Concept of Law. *Oxford Journal of Legal Studies*, Vol. 24(4), p. 717). Other authors also agree that the law depends on facts: „However, legal practice and theory of legal interpretation shows that the facts influence the content of the law" (Spruogis, E. (2006). Problematic Aspects of Law Interpretation, *Jurisprudencija. Mokslo darbai*, 8(86), p. 57).

[2] *Libert v. France*, no. 588/13, 22 February 2018.

[3] *Peck v. the United Kingdom*, no. 44647/98, ECHR 2003-I.

[4] *Uzun v. Germany*, no. 35623/05, ECHR 2010 (extracts).

[5] *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 96, ECHR 2012.

[6] *Eerikäinen and Others v. Finland*, no. 3514/02, § 70, 10 February 2009.

[7] See, for example, *Douglas v. Hello!* (No 3) [2005] EWCA Civ 595; [2005] 3 W.L.R. 881, at 106 in which Lord Phillips M.R. said: "Nor is it right to treat a photograph simply as a means of conveying factual information. A photograph can

Thus, it could be said that filming (photographic) devices, such as unmanned aerial systems (hereinafter – *UAS*/drones), closed-circuit television cameras (hereinafter – *CCTV* cameras), dashboard cameras (car cameras), photo-video-cameras (hereinafter all such and similar devices called – visual information recording devices/*VIRDs*) are the best tool for the collection of the most accurate information and, accordingly, for intentional or not - the breach of someone's right to respect for private life.

As "privacy is an issue of profound importance around the world"[8] and "there appears to be [a] worldwide consensus about the importance of privacy and the need for its protection",[9] state's attitude towards privacy protection in this field is very important, especially having in mind rapid technological developments (for example, the growing use of facial recognition technologies),[10] people's growing financial possibilities which only mean that *VIRDs*, such as *UASs*, dashboard cameras or *CCTV* could be owned by each individual in the nearest future[11] (the same, what happened with mobile phones that earlier were a thing of luxury but after a couple of decades they have become a necessity of every adult). Thus, the states' vision of a long-term strategy of controlling and organising such use is significant. The quality of legal regulation is essential as the current regulation is only a temporary solution. In order to achieve effective regulation, interests, such as economic, security, privacy must be harmonized, in other words, the states must have a systematic approach to the issue. That is to say, regulation of the use of *VIRDs* must be clear and reasonably improving, the requirements for such use should be proportionate realistic, at the same time – effective.

The topicality, novelty, and practical use of the research. Even though the Council of Europe and the European Union had started to set the basis of privacy protection respectively seventy years and a couple of decades ago,[12] but it seems that perception of how valuable privacy is together

certainly capture every detail of a momentary event in a way which words cannot, but a photograph can do more than that. A personal photograph can portray, not necessarily accurately, the personality and the mood of the subject of the photograph".

[8] Solove, D. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press, p. 2.

[9] Pranevičienė, B. (2011). Limiting of the Right to Privacy in the Context of Protection of National Security. *Jurisprudence*, 18(4), p. 1613.

[10] Nesterova, I. (2020). Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world. *SHS Web of Conferences* 74(03006) (2020), p. 2.

[11] Chongqing, a city in China, has one CCTV camera for every 5.9 citizens—or 30 times their prevalence in Washington, D.C. (Campbel, Ch. (2019, 21 November). 'The Entire System is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World. Retrieved 25.12.2019 from https://time.com/5735411/china-surveillance-privacy-issues/).

[12] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Published: OJ *L 008, 12.01.2001, pp. 0001 - 0022.* Ceased to be in force.

with the adoption of *GDPR*[13] has come into people's lives so suddenly that made everybody rethink about the importance and weight of this right. Although according to the *EU* (hereinafter called – the *EU*) law, personal data is protected by a separate right from privacy,[14] it is obvious that these rights are closely related and sometimes overlapping, therefore it is impossible not to mention the protection of personal data and not to associate it with privacy in this research. Since the *GDPR* came into force, without any exaggeration, quite a big confusion could be felt in private businesses and establishments, whereas natural persons started wondering what private information connected with them was collected, processed, or had been accessible by other subjects. The notices received by e-mails and text messages asking whether people wished to continue receiving adverts, personalised offers, minded everybody that things which had been happening for years were a continuous infringement of the use of their personal data. Along with this understating, considerations on what the other contexts of the breaches of people's right to protection of personal data, privacy are. It seems like society has become more alert and more respectful of privacy.

GDPR protects personal data (which serves for the protection of privacy) when it is processed by business entities but it is not necessarily so when personal data is processed by natural persons. One of the exceptions of application of *GDPR* enshrined in its Article 2 part 2 clause c ("This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity") means that the application of *GDPR* in cases when personal data is processed by a natural person requires additional assessment which, as the research will show, will most probably lead to a situation when *GDPR* cannot be invoked. As *GDPR* is quite a complex and even confusing legislation, application of it in the relationship between natural persons in the context of data processing for personal and household activities would be disproportionate. So, this is when national laws must be invoked. However, if they are not efficient, sufficient, and proportionate, regulatory gaps are faced.

One of the spheres in which the term "privacy" is mentioned very often is the use of visual information recording modern technology. It is important that neither in Latvian nor in Lithuanian legal doctrine the topic of privacy protection in the use of visual information recording devices has been analysed a lot. The novelty of the research is determined by the fact that dashboard cameras, *UASs*, as visual information recording devices have become so popular not very long time ago, the

[13] 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). Published: OJ L 119, 4.5.2016, pp. 1–88.
[14] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. Published: OJ C 326, 26.10.2012, pp. 391–407.

states only since 2014 and 2016, respectively Lithuania and Latvia, have been creating the legal basis for operation and use of *UASs*. Whereas special regulation on *CCTV* cameras and dashboard cameras does not even exist in any of the two countries. While there is a growing focus on perceptions of *UASs* more generally but the studies do not fully address privacy. There is little information regarding the nexus between *UASs* and privacy. This is a notable gap in the literature given the growing use of *UASs*, particularly among private users, and the potential for significant privacy violations.[15] The use of various *VIRDs* by natural persons is only increasing but the situation with regulation concerning their use has not changed much, except for the regulation at the *EU* level (only on June 11 of 2019 Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft[16] (hereinafter called – *Regulation 2019/947*) entered into force) which proves the novelty and the necessity of the research. Taking into consideration that Member States will have to align national regulation with the *EU* law, as well as to legally regulate the use and operation of other *VIRDs*, such as dashboard cameras, the research could be useful for state governments as pointing problematic aspects of current regulation and in such a way helping to avoid the creation of faulty national regulation by learning from the neighbor's mistakes or positive examples. Moreover, Latvian scholars summarise that the existence of a regulatory framework, as well as legal research conducted in this area in Latvian legal doctrine, does not suggest that Latvia has a clear understanding of privacy as a single protected benefit and its content yet.[17] Therefore analysis related to this institute is timely and necessary in Latvia as well. Finally, a comparison between the regulation of the two states allows systematically evaluate the regulatory characteristics of both states. For these reasons, the research is useful in achieving more effective regulation of privacy protection in the field of the use of *VIRDs*.

Besides the abovementioned regulation by the European Union in the data protection field (*GDPR*), great recent work of the European Union Aviation Safety Agency in regulating the operation of drones – the adoption of new regulation[18] which stresses the protection of privacy and determines real measures to ensure this value – also proves topicality of the research – urgent demand of clear regulation of the operation of modern technologies. The lack of such regulation may lead to massive violations of the right to respect for private life, therefore, it is necessary to raise questions on the

[15] Nelson, J. R., Grubesic, T. H., Wallace, D., Chamberlain, A. W. (2019). The View from Above: A Survey of the Public's Perception of Unmanned Aerial Vehicles and Privacy. *Journal of Urban Technology*, Vol. 26(1), p. 84-85.
[16] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance). Published: OJ L 152, 11.6.2019, pp. 45–71.
[17] Torgans, K., Karklinš, J. and Bitans, A. (2017). *Ligumu Un Deliktu Problemas Eiropas Savieniba un Latvija* (Contract and Tort Problems in the European Union and Latvia). Riga: Tiesu namu agentūra, p. 352.
[18] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance). Published: *OJ L 152, 11.6.2019, pp. 45–71.*

sufficiency of such regulation, and, if it is found that national regulation on the operation and use of visual information recording devices by various subjects (legal and natural persons – for various purposes) is not sufficient, improve, adjust or create it. However, it is also important to determine whether the regulation is not too restraining technological development as the latter's necessity is undeniable and inevitable. This is an important factor to consider when legislating.

The research showed that in terms of privacy protection currently existing *EU* regulation on the use of *UASs* and on data protection is either ineffective or unclear, whereas Lithuanian jurisdiction is lacking more detailed, clear regulation concerning the operation and use of *UASs*. Furthermore, special regulation concerning dashboard cameras does not even exist in the chosen jurisdiction, protection of people's right to their image, personal data is unclear and insufficient as well. An example of the Gatwick airport drone incident proved that national authorities do not even know how to deal with the threats caused by modern technologies, as there is no regulation allowing the officials to act against violations these technologies cause.[19] Therefore state regulation has to not only reflect, for example, generally applicable *EU* regulations on the prevention of various threats that could be caused by modern technologies but also to ensure effective remedies to tackle the breaches that have already been committed. For this reason, it is necessary to systematically investigate how privacy protection is ensured in a particular national jurisdiction in the field of the operation and use of visual information recording devices. Such analysis is relevant because national jurisdictions are constantly confronted with challenges caused by modern technologies (particularly, *VIRDs*), the disputes concerning their use are only maturing, and new questions of legal governance of *VIRDs*' operation and use arise.

State regulation is the only effective tool to protect people's privacy from possible threats therefore it is essential to make sure it is effective and sufficient.

Research object: Lithuanian regulation of privacy protection in the use of *VIRDs* by natural persons. Lithuania is a member of the *EU*, it is also a signatory party of various international treaties and conventions, related to privacy protection, including the European Convention on Human Rights,[20] therefore the country is bound by the privacy rules and their interpretation that have been

[19] The airport had to be closed for 30 hours, leading to the cancellation of more than 1,000 flights affecting 140,000 passengers affected, after numerous reported drone sightings. The overall police investigation cost a total of £790,000 but in December 2019 has been closed without anybody being charged (Evans, M. (2019, 26 September) Gatwick Airport Drone Investigation Closed By Police Without Anyone Being Charged, retrieved 10.10.2019 from https://www.telegraph.co.uk/news/2019/09/26/gatwick-drone-investigation-closed-without-suspect-identified/.

[20] Convention for the Protection of Human Rights and Fundamental Freedoms. Signed in Rome 04.11.1950. Latvia joined the treaty on 27.06.1997. Law "On European Convention for the Protection of Human Rights and Fundamental Freedoms 4th November 1950 and its protocol 1st, 2nd, 4th, 7th and 11th protocol." Published Latvijas Vestnesis, 143/144, 13.06.1997.

formulated by the *EU* and international instruments (the treaties, conventions, and case-law of international courts). For this reason, the research includes not only the analysis of state regulation concerning privacy protection in Lithuania, which is/could be applicable in cases of the use of *VIRDs* by natural persons but also international and *EU* regulation on privacy protection and case-law of international courts.

The research does not encompass analysis of the use of *VIRDs* by natural persons for business purposes, as such data processing could be equated to the data processing by business entities and falls under the scope of *GDPR*. Meanwhile, *GDPR* is analysed only in the aspects that concern data processing by natural persons, not for business purposes.

For the purpose of the practical applicability of the research, various aspects analysed are parallelly compared with Latvian ones. Such comparison is also intended to help to achieve the research goal, as by comparing national regulation with other state's national laws shortcomings could be determined more easily.

VIRD in the research means any type of device which is capable of recording video (for example, *CCTV* camera, dashboard camera) any photographic equipment (such as photo cameras or mobile phones with integrated photo-cameras, unmanned aerial vehicles (drones) (equipped with video/photo cameras). However, the author of the research sometimes stresses a particular device because of its special characteristics worth consideration. In such a case that special device is named separately.

For clarity, it is necessary to stress that the *VIRDs* mentioned above all have functions of not only video recording but also taking photographs, therefore hereinafter these two functions (photography and video) are treated as the same regardless of which function is mentioned unless the context allows only precise function.

The research analysis covers regulation on both: use of *VIRDs* and privacy protection in civil, administrative, and criminal laws (if these privacy protection rules could be applicable in the use of *VIRDs*).

The author of the research does not analyse problems related to privacy protection in the processing of biometric data because the processing of such type of data requires biometric systems. Such systems are very complex (they contain a signal detection system with a pattern recognition architecture which is capable of sensing a raw biometric signal, processing this signal to extract a salient set of features called biometric identifier or template and comparing these features against the

ones stored in the database[21]), processing of biometric data is usually undertaking a wide scope of personal data subjects and its use requires further steps and techniques than capturing visual information. For these reasons, it is not probable that it could be processed by natural persons, not for business purposes. Furthermore, as biometric data is a very complex process its in-depth analysis would require another research.

Research goal: Determine dysfunctions of Lithuanian regulation of privacy protection in the use of *VIRDs* and suggest possible and effective remedies.

In order to achieve the goals defined, the following **tasks** have been set in the research:

1. To describe the impact of modern technologies on human rights.
2. To introduce the specificity and importance of *VIRDs* as technical means and describe their main principles of use and operation,
3. To describe subjects of the use of *VIRDs* in terms of their status and purpose of the use.
4. To describe and analyse the content of the right to respect for private life by reviewing international, *EU*, and state regulation and case-law related and applicable in the context of the use of *VIRDs*.
5. To describe, systematically analyse, and compare state regulation (Latvian and Lithuanian) related specifically to the use of *VIRDs* with a focus on privacy protection and to assess the shortcomings of such regulation.

Research question. Is Lithuanian state regulation on the use of *VIRDs* sufficient for the effective protection of privacy in this field?

Structure of the research. The work consists of an introduction, five parts, and conclusions.

1. The introduction includes a description of a problem and justification of topicality of the theme, also the research object, goals, tasks set, research question, limitations, methodological aspects of the research and methods, the scientific novelty of the research, its practical significance, previous research work and dissemination of the doctoral research results are defined in it.
2. The first chapter of the research describes modern technology's impact on privacy, deals with the questions of the specificity of *VIRDs*, their use as well as subjects of the use of *VIRDs* in terms of their status and the purpose of the use are described.
3. In the second chapter, the right to respect for private life and, accordingly, the concept of privacy is analysed, summarized theoretical aspects of the right as enshrined in international and the European Union legislation and explained by international courts in their case-law. Only the

[21] Jain, A., Ross, A., Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, Vol. 1(2), p. 128.

aspects relevant to the analysis of privacy protection in the use of *VIRDs* are mentioned, excluding the ones which are not. Also, Latvian and Lithuanian state regulation on various aspects of privacy, which in any way could be used in governing the use of *VIRDs* (including operation of particular kind of *VIRD* governing laws, or by-laws) is described.

4. The third chapter includes specific privacy-*VIRDs*-related aspects, such as description and the content of the concept "home", the right to the protection of one's image, "household exemption" used in the laws related to privacy protection.

5. The fourth chapter is dedicated to the analysis of problematic aspects of the regulation described in the previous chapter and other problems. The regulatory gaps are disclosed through the modelling as well as the examples of how privacy could be defended in a particular situation and the suggestions on how the shortcomings of the current regulation could be fixed, are given.

6. The fifth chapter contains the discussion on the balance between privacy protection and freedom to use modern technologies.

The theoretical and methodological base for the research consists of international, European Union, and national (Lithuanian, as well as Latvian – for comparison - regulatory enactments, *ECHR*, *ECJ* (hereinafter – European Court of Justice), and national court's case-law, monographs developed by legal scholars, publications, and Internet resources.

The importance of the research has been disclosed by emphasizing the impact of modern technology on human rights. Here the doctrinal works of Abulashvili, V.,[22] Myers, J. M.,[23] Lauren, P. G.[24] were used.

The amount of various research on the privacy topic is abundant. The most helpful for disclosure of the essence of privacy concept was *ECHR* case-law, however, the works of Merrills, J.G., Robertson, A.A.,[25] Griffin, J.[26] Michael, J.,[27] K.Ziegler,[28] Juliane Kokott, and Christoph

[22] Abulashvili, V. (2018). Human Rights and Development of Technology. *L'Europe Unie/United Europe*, Vol. 12/2018, p. 47.
[23] Myers, J. M. (1998). Human rights and development: Using advanced technology to promote human rights in sub Saharan Africa. *Case Western Reserve Journal of International Law*, Vol. 30, p. 343.
[24] Lauren, P. G. (2011). *The Evolution of International Human Rights: Visions Seen (3rd edn.)*. Pennsylvania: University of Pennsylvania Press, p. 3 13.
[25] Merrills, J.G., Robertson, A.A (2001). *Human Rights in Europe: Study of the European Convention on Human Rights (4th edn.).* Manchester: Manchester University Press, p. 362.
[26] Griffin, J. (2009). *On Human Rights*, New York: Oxford University Press, p. 239.
[27] Michael, J. (1994). *Privacy and Human Rights: International and Comparative Study, with Special Reference to developments information technology*. Dartmouth: Unesco Publishing, p. 194.
[28] Ziegler, K. (2016). The Relationship between EU Law and International Law. *A Companion to European Union Law and International Law*, New York, United States: John Wiley & Sons Inc, pp. 42-61.

Sobotta,[29] Fernando Volio,[30] Krastiņš, U., Liholaja, V.,[31] N. Taylor,[32] P. Hert,[33] U. Kilkelly, [34] K. Jovaišas,[35] L. Meškauskaitė,[36] A. Vosyliūtė,[37] Torgans, K., Karklinš, J. and Bitans, A.[38] , as well as quite a deep analysis of privacy carried out by N. A. Moreham, helped to create an overall picture of the concept in the context of *VIRDs* use. The abundance of sources related to privacy proves that the question of privacy has been and still is topical.

On the other hand, even though the topic of *CCTV* cameras, their use (especially for crime prevention) has been also quite popular among scholars (La Vigne, N.[39], and Lowry, S., Welsh, B. C., and Farrington, D. P., [40] Munyo, I., Rossi, M.,[41] Alexandrie, G.,[42] Weaver, B., Lahtinen, M.,[43] Piza, E.L., Caplan, J.L., Kennedy, L.W.[44]) it could not be said so about scholarly works (scientific

[29] Kokott, J., Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, Vol. 3(4), pp. 222-228.
[30] Volio, F. (1981). Legal personality, privacy and the family. *The International Bill of Rights: The Covenant on Civil and Political Rights*. New York: Columbia University Press, pp. 190-193.
[31] Krastiņš, U., Liholaja, V. (2016). *Krimināllikuma komentāri. Otrā daļa (IX-XVII nodaļa)*. Rīga: Tiesu namu aģentūra, p. 560.
[32] Taylor, N. (2002). State Surveillance and the Right to Privacy, *Surveillance & Society*, Vol. 1(1), pp. 66-85.
[33] Hert, P. (2005). Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11. *Utrecht Law Review*, Vol. 1(1), pp. 68-96.
[34] Kilkelly, U. (2003). The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights. *Human Rights Handbooks Series*, Vol., p. 72. Retrieved 01.17.2016 from https://rm.coe.int/168007ff47.
[35] Jovaišas, K. (2005). Žmogaus būsto neliečiamumo teisinis režimas. *Teisės problemos*, Vol. 2(48).
[36] Meškauskaitė, L. (2015). *Teisė į privatų gyvenimą*. Vilnius: VĮ "Registrų centras", p. 336.
[37] Vosyliūtė, A. (2008). Įsibrovimo į patalpą, saugyklą ar saugomą teritoriją kaip vagystę kvalifikuojančio požymio samprata teisės moksle ir teismų praktikoje ("The concept of trespassing premises, storage or secured territory as elements of aggravated theft under the theory of law and practice"). *Teisė* 66(1), pp. 75-94.
[38] Torgans, K., Karklinš, J. and Bitans, A. (2017). *Ligumu Un Deliktu Problemas Eiropas Savieniba un Latvija* (Contract and Tort Problems in the European Union and Latvia). Riga: Tiesu namu agentūra, pp. 414.
[39] La Vigne, N., & Lowry, S. (2011). Evaluation of camera use to prevent crime in commuter parking lots: A randomized controlled trial. Washington, DC: Urban Institute, Justice Policy Center. Retrieved 14.10.2018 from https://www.ncjrs.gov/pdffiles1/nij/grants/236740.pdf.
[40] Welsh, B. C., & Farrington, D. P. (2008). Effects of closed circuit television surveillance on crime. *Campbell Systematic Reviews*, Vol. 17, 1–73.
[41] Munyo, I., Rossi, M. (2016). Is it displacement? Evidence on the impact of police monitoring on crime (Working Paper No. 126). Retrieved 04.10.2019 from http://www.ridge.uy/wp-content/uploads/2016/05/Rossi_Martin.pdf; Gómez, S., Mejķa, D., Tabón, S. (2017). The deterrent effect of public surveillance cameras on crime (Working paper No. 9). Retrieved 05.10.2019 from: https://economia.uniandes.edu.co/components/com_booklibrary/ebooks/dcede2017-09.pdf
[42] Alexandrie, G. (2017). Surveillance cameras and crime: a review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, Vol. 18(2), p. 217.
[43] Weaver, B., Lahtinen, M. (2016). Kameraövervakningens effekter – vad vet vi och vad vet vi inte? [The effects of video surveillance – What we know and what we don't know]. *Övervakning och integritet: Teknik, skydd och aktörer i det nya kontrollandskapet [Surveillance and integrity: Technology, protection and actors in the new control landscape]*. Stockholm: Carlsson Bokförlag, recited from Alexandrie, G. (2017). Surveillance cameras and crime: a review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, Vol. 18(2), p. 221.
[44] Piza, E.L., Caplan, J.L., Kennedy, L.W. (2014). Analyzing the Influence of Micro-Level Factors on CCTV Camera Effect. *Journal of Quantitative Criminology*, Vol. 30, p. 238.

publications) related to other *VIRDs*, such as dashboard cameras and *UASs*. It proves that the topic is not exhausted yet. Therefore, the author of the research analysed legal international, *EU*, and national (Latvian and Lithuanian) legal enactments on the governance of the use of these devices and related privacy protection rules.

The benefits of *VIRDs* have been analysed by using the works of the following authors: J.Villasenor[45], Martin McKown[46], Kavoosi, Z., Hossein Raoufat, M., Dehghaani, M., Jafari, A., Kazemeini, A., Jafar Naazemossadat, M., [47] A.G. Entrop and A. Vasenev[48], Dupont, Q. F. M., Chua, D. K.H., Tashrif, A., Abbott, E. L.S[49], Khan, M. A., Ectors, W., Bellemans, T., Ruichek, Y., Yasar, A. H., Janssens, D., Wets, G. [50], Rogavichene, L., Garmonnikov, I.,[51] Nauwelaerts, W. [52] These authors have analysed the usage of visual information recording devices in a surprising variety of areas which only proves that balancing between privacy protection and development of modern technologies is of great importance. Comparison of national legal enactments was carried out through entire research which helped to disclose peculiarities, gaps, and advantages of the national regulations.

The admissibility of the above-mentioned scholarly works of foreign legal scholars and lawyers and the use of international courts' practice, as well as international and European Union legislation is not only justified but unavoidable and necessary as both countries – Latvia and Lithuania – are parties of various international treaties and also members of the European Union. Thus, for proper and comprehensive analysis these sources could not be ignored.

---

[45] Villasenor, J. (2013). Observations from Above: Unmanned Aircraft Systems and Privacy. *Harvard Journal of Law & Public Policy* 36, pp. 457-517.

[46] McKown, M. (2015). The New Drone State: Suggestions for Legislatures Seeking to Limit Drone Surveillance by Government and Nongovernment Controllers. *University of Florida Journal of Law and Public Policy*, Vol. 26, pp. 71–90.

[47] Kavoosi, Z., Hossein Raoufat, M., Dehghaani, M., Jafari, A., Kazemeini, A., Jafar Naazemossadat, M., (2020). Feasibility of satellite and drone images for monitoring soil residue cover. *Journal of the Saudi Society of Agricultural Sciences*, Vol. 19(1), pp. 56-64.

[48] Entrop, A.G., Vasenev, A. (2017). Infrared Drones in the Construction Industry: Designing a Protocol for Building Thermography Procedures, *Energy Procedia*, Vol. 132, pp. 63-68.

[49] Dupont, Q. F. M., Chua, D. K.H., Tashrif, A., Abbott, E. L.S. (2017). Potential Applications of UAV along the Construction's Value Chain. *Procedia Engineering*, Vol. 182, pp. 165-173.

[50] Khan, M. A., Ectors, W., Bellemans, T., Ruichek, Y., Yasar, A. H., Janssens, D., Wets, G. (2018). Unmanned Aerial-Vehicle Based Traffic Analysis: A Case Study to Analyze Traffic Streams at Urban Roundabouts. *Procedia Computer Science*, Vol. 130, pp. 636-643.

[51] Rogavichene, L., Garmonnikov, I. (2017). Innovative Technologies for Assessment and Correction of the Driving Style. *Transportation Research Procedia*, Vol. 20, pp. 564-570.

[52] Nauwelaerts, W. (2014). *Guidelines on Use of Dashboard Cameras Published by Belgian Privacy Commission*, World Data Protection Report: Guidelines on Use of Dashboard Cameras, Vol. 14(2). Retrieved 06.05.2018 from https://www.hunton.com/files/Publication/a75c66a4-2f6f-4e3e-a83b-543923987393/Presentation/PublicationAttachment/580a5a0c-66f6-4cee-834c-8b41b637fd09/Guidelines_on_Use_of_Dashboard_Cameras.pdf

As the problem raised in the research is quite new (because the use of *VIRDs* has become quite common only relatively recently), national courts are not rich with cases related to the defence of privacy in the context of the use of *VIRDs*. Only a few topical cases were found and they only helped to evaluate the effectiveness of national compensatory mechanisms in the field of *VIRD*-related privacy breaches.

Dissemination of the doctoral research. The main results and insights of the research have been delivered in four scientific articles written in English and published in scholarly journals. "Regulation of unmanned aerial systems and related privacy issues in Lithuania", published in the "Baltic Journal of Law and Politics"[53] encompassed analysis of regulation on *UASs* and related privacy issues in Lithuania. Another scientific article, published in the journal "Problems of Legality" was connected with an analysis of whether visual information recording devices were more good than a threat.[54] The third article was devoted to the analysis of the new *EU* regulation on *UASs* and published in "Public Security and Public Order".[55] The fourth article "State regulation of privacy and its protection in the use of VIRDs by police: comparative perspective from Latvia and Lithuania" was published in "Public Security and Public Order"[56] and was analysing aspects of privacy protection in the use of visual information recording devices in the police.

The author of the research has made six presentations related to the topic of the dissertation in the following conferences: 1) Unmanned Aerial Systems: A Threat to Privacy? Conference "Problems on Ensuring Public Security: Theoretical and Practical Aspects" held on the 12'th of April 2018, Kaunas, Lithuania; 2) Legal Regulation of the Image Capturing Devices: Balancing Between Societal Security and Threat to Privacy. Conference "Problems on Ensuring Public Security: Theoretical and Practical Aspects" held on the 9'th of May 2019, Kaunas, Lithuania; 3) Image Capturing Devices: Threat or Good? Conference "Society. Integration. Education", held on the 24'th of May 2019, Rezekne, Latvia; 4) International, the European Union and State Regulation of Privacy Protection in the Use of ICDs. Conference "Networking on Sustainable Security in Dynamic Environment", held on the 20'th of October 2020, Kaunas, Lithuania; 5) Privacy Protection in the Use of Visual Information Recording Devices by Police. Conference "Networking on Sustainable Security in the

[53] Pūraitė, A., Bereikienė, D., Šilinskė, N. (2017). Regulation of unmanned aerial systems and related privacy issues in Lithuania. *Baltic Journal of Law & Politics*, Vol. 10(2), pp. 107-132. doi: 10.1515/bjlp-2017-0014

[54] Pūraitė, A., Šilinskė, N. (2019). Image capturing devices: threat or good. *Problems of Legality*, Vol. 144, pp. 120-137. doi: 10.21564/2414-990x.144.157226

[55] Pūraitė, A., Šilinskė, N. (2020). Privacy protection in the new EU regulations on the use of unmanned aerial systems. *Visuomenės saugumas ir viešoji tvarka*, Vol. 24, pp. 173-183. doi: 10.13165/PSPO-20-24-11

[56] Pūraitė, A., Šilinskė, N. (2021). State regulation of privacy and its protection in the use of VIRDs by police: comparative perspective from Latvia and Lithuania. *Visuomenės saugumas ir viešoji tvarka*, Vol. 27, pp. 115-132. doi: 10.13165/PSPO-21-26-32

Dynamic Environment", held on the 20'th of April 2021, Kaunas, Lithuania; 6) Visual Information Recording Devices and the Charades of Their Legal Assessment. Conference "Security & Forecasting 2021 Sec4", held on 11'th May 2021, Warsaw, Poland.[57]

Research methods. The research was prepared using qualitative[58] research techniques (methods) formulated in legal doctrine.[59] They helped to disclose the essence of the research, to achieve the goal of the study, and to fulfill the tasks set.

By the method of ***document analysis,*** Latvian and Lithuanian state regulations were analysed, also national and international case-law related to privacy protection in the use of *VIRDs*. The method laid the foundations for further analysis and completion of the tasks set.

The descriptive method allowed the author to define *VIRDs* considering their specificity, to determine the essence of the privacy concept.

The analytical-critical method was used to evaluate the quality of state regulation concerning privacy protection in the use of *VIRDs*, also to determine the shortcomings of such regulation.

The method of ***scientific literature analysis*** allowed the author of the research to delve deeper into the significance of the *VIRDs*, to better understand and summarise the interpretations of the privacy concept.

The method of ***systematic analysis*** promotes a systematic approach to the subject of the research, therefore it helped to get an overview of the situation in state regulation of the use of *VIRDs* and to comprehend the problematic aspects of the regulation which allowed to suggest appropriate corrections and make the conclusion.

[57] Pūraitė, A., Šilinskė, N. Unmanned Aerial Systems: A Threat to Privacy? Conference "Problems on Ensuring Public 'Security: Theoretical and Practical Aspects" held on the 12'th of April 2018, Kaunas, Lithuania; Šilinskė, N. Legal Regulation of the Image Capturing Devices: Balancing Between Societal Security and Threat to Privacy. Conference "Problems on Ensuring Public Security: Theoretical and Practical Aspects" held on the 9'th May 2019, Kaunas, Lithuania; Pūraitė, A., Mikalauskaitė, K., Šilinskė, N. Image Capturing Devices: Threat or Good? Conference "Society. Integration. Education", held on the 24'th May 2019, Rezekne, Latvia; Šilinskė, N. International, the European Union and State Regulation of Privacy Protection in the Use of ICDs. Conference "Networking on Sustainable Security in Dynamic Environment", held on the 20'th of October 2020, Kaunas, Lithuania; Šilinskė, N. Privacy Protection in the Use of Visual Information Recording Devices by Police. Conference "Networking on Sustainable Security in the Dynamic Environment", held on the 20'th of April 2021, Kaunas, Lithuania; Šilinskė, N. Visual Information Recording Devices and the Charades of Their Legal Assessment. Conference "Security & Forecasting 2021 Sec4", held on 11'th May 2021, Warsaw, Poland.

[58] Qualitative research technique – conscious search of particular methods and approaches, the characterization of qualitative features of social phenomena, processes and systems.

[59] Method – the path of research, mode of cognition: 1. Consciously and in a certain sequence applied way of pursuit of purpose. 2. A way of studying nature and social life to organise and justify system of knowledge. Осипов, Г.В. (ред.) (1998). *Социологический энциклопедический словарь*. Москва: НОРМА, p. 177; Tidikis, R. (2003). *Socialinių mokslų tyrimų metodologija*. Vilnius: LTU, 2003, p. 190.

The method of ***modelling*** was the tool that helped by describing real-life-alike situations to illustrate the problems of the current regulation and demonstrated which areas the changes must be done in.

The comparative method helped to disclose the differences and similarities between Latvian and Lithuanian state regulations on the use of *VIRDs*. The application of this method helped to complete the task to compare state regulation which set the basis for the further analysis and completion of other tasks – to assess and find the shortcomings of such regulation.

The method of ***source content analysis*** was used to analyse foreign and national legislation and research works.

The methods described influenced the interpretation of various sources used in the research, also made a great influence on the implementation of the tasks and goals set herein, accuracy, validity, and reliability of the conclusions and generalizations made.

A concise description of the doctoral thesis by chapters. Hereinafter short description of the contents of the chapters of the thesis is described.

Introduction. The introduction of the doctoral thesis defines a description of a problem, the topicality, novelty, and practical use of the research, research object and limitations, goals, and tasks, research question, structure, the theoretical and methodological base for the research, dissemination of the doctoral research and scientific research methods used.

The 1st chapter: "Theoretical dimension of modern technology: impact on human rights, the specificity, and benefits of visual information recording devices". The chapter is dedicated to discussing questions that help to understand the context of the research: general aspects of the interaction between human rights and new technologies are discussed (sub-chapter 1.1), visual information recording devices, their specificity, and benefits are described (subchapters 1.2 and 1.3), classification of VIRDs' users is presented (sub-chapter 1.4).

The main problem in the context of modern technology is the evolutionary gap that occurs between technical progress and legal implementation procedures. To be more precise, scholars find national and international rules to advances in science and technology being too slow and consequently inadequate to regulate new legal situations created by the developments of the latest technological innovations.[60] Therefore it is essential that governments' actions are timely and effective. Reality is not static, an innovative evolution being in endless motion is identified, therefore the purpose of the law is to observe all the changes and to adjust them to the new situation generated

[60] Coccoli, J. (2017). The Challenges of NewTechnologiesin the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era. *Peace Human Rights Governance*, Vol. 1(2), p. 224.

every time.[61] Thus, among the most important actions that national legislations must take in order to harness the opportunities of new technologies is the "creation of adequate legal frameworks and mechanisms to ensure full accountability in the context of new technologies, including by reviewing and assessing the gaps in national legal systems, creating oversight mechanisms, where necessary, and making available avenues for remedies for harm caused by new technologies",[62] so that new technologies contributed to the full enjoyment of human rights by all, including economic, social and cultural rights, and adverse impacts on human rights were prevented.[63]

Description of the benefits of VIRDs proves that the idea of the necessity for the law to go side by side with new technological developments is correct as there is a great number of advantages that these technologies have. This must be taken into consideration when balancing privacy protection and the regulation on the use of modern technologies. However, the characteristics of VIRDs "activate the alarm" when talking about the threat to privacy they cause. VIRDs' abilities, such as unobtrusively getting into private territories, or secret filming, processing huge amounts of private information, personal data require special attention from legislators.

The users of *VIRDs* by their status in terms of subordination could be divided into governmental and non-governmental users, whereas the latter sub-categorized into natural persons and business entities. The purposes that natural persons could use *VIRDs* are recreational, self-protection purposes, and illegal, whereas business entities could use *UASs* for commercial and illegal purposes. The most important difference among all these types of private information collectors is that depending on their status and the purpose of the collection of private information, different legal tools to tackle the offence have to be used.

The 2nd chapter: "Legal dimension of privacy and its protection in the use of VIRDs: international, the European Union, and state regulation". This chapter is divided into five sub-chapters dedicated to discussing international, EU, and state regulation in privacy.

Sub-chapter 2.1 speaks about the complexity of the concept of privacy. An extraordinary beginning of the right (it was first established at the international law than in fact was fully protected

[61] Karanasiou, A. P. (2012). Respecting Context: A New Deal for Free Speech in the Digital Era. *European Journal of Law and Technology*, Vol. 3(3), p. 1, online version: https://ejlt.org/index.php/ejlt/article/view/144/266.
[62] Human Rights Council of the United Nation (2020). *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights (advance edited version), retrieved 14.02.2021 from* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf, p.15.
[63] Human Rights Council of the United Nation (2020). *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights (advance edited version), retrieved 14.02.2021 from* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf, p. 15.

by any domestic constitutional system) gave rise to the problematics of its further development (as the right did not have its deep roots in national jurisdictions and the realization of this right was not mature in the human subconscious). Even though the right to respect for private life, the right to privacy is enshrined in so many conventions and other international and nowadays - national legal acts, it is still not well defined and is nowhere stated precisely in any human rights code.[64]

The following sub-chapter (2.2) includes a description of privacy in international legislation and case-law. Thus, not only the main international legal acts on privacy protection are mentioned, but also the rules of privacy protection, that could be applicable in the use of VIRDs, formulated by ECHR in its case-law are described (including the doctrine of margin of appreciation).

Sub-chapter 2.3 contains an analysis of privacy protection in the use of VIRDS in the EU legislation, discusses the relationship between privacy and personal data, and touches special regulation on the use of UASs (i.e. specific aspects of Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, related to privacy protection). Because in the past few years great attention to the protection of personal data, privacy, and drone use regulation has been paid in the European Union, it could be said that for the Member States of the *EU* the most detailed regulation on the protection of privacy when using *UASs* also data protection is set at the European Union level. Thus, taking into consideration the wide scope of national addresses of the main *EU* law enshrining privacy protection, and that the case-law of *ECJ* could also be treated as „binding additional legal source"[65] regulation at the *EU* level has a significant impact on the creation of national laws and their implementation.

Sub-chapters 2.4 and 2.5 are related to the analysis of state regulation on privacy protection of Lithuania and Latvia respectively and disclose peculiarities of privacy protection in civil,

[64] Robertson, D. (2004). *A Dictionary of Human Rights (2nd edn.)*. London and New York: Europa Publications, p. 179; Warren, S. D., Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4(5), p. 193; Post, R. C. (2000-2001). Three Concepts of Privacy. *The Georgetown Law Journal*, Vol. 89, p. 2087; Whitman, J. Q. (2004). The Two Western Concepts of Privacy: Dignity versus Liberty. *Yale Law Journal*, Vol. 113, p. 1153; Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, Vol. 90, p. 1089; Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Vol. 154(3), p. 479; Griffin, J. (2007). The Human Right to Privacy. *San Diego Law Review*, Vol. 44(4), p. 717.

[65] Mikelsone, G. (2013). The Binding Force of the Case Law of the Court of Justice of the European Union. *Jurisprudence*, Vol. 20(2), p. 474; Dupate, K. (2011). Case Law of the Court of Justice of the European Union (Eiropas Savienības Tiesas Prakse Darba Tiesībās). Retrieved 27.04.2020 from https://arodbiedribas.lv/wp-content/uploads/2019/11/es_tiesas_prakse_darba_tiesibas.pdf.; Mikelsone has also stressed that "The case law of the ECJ is also applied by Latvian courts that consider it to be a binding legal source <…> The Department of Civil Cases of the Senate, the Supreme Court of the Republic of Latvia (hereinafter the DCC of the Senate), in its judgment of 14 October 2009 in the Case No.SKC-899 decided the case (the judgment of 20 April 2009 given by the Civil Division of Riga Regional Court was in part set aside) on the basis of the interpretation of provision made in Article 28 of the ECJ judgment of 09.02.1999 in the Case C-167/97, *Regina v. Secretary of State for Employment* (the judgment of 14 October 2009 given by the DCC of the Senate in the Case No.SKC-899, para. 10.2, 10.2.1, 10.2.2, 10.2.4, 10.2.5)."

administrative, and criminal laws and provides a comparison of privacy protection in these two jurisdictions.

The 3rd chapter: "Other aspects of the protection of privacy in the use of VIRDs and related shortcomings". The content of the third chapter is laid out in three sections. Section 3.1 undertakes an analysis of relevant aspects of the right to the protection of one's image in the use of *VIRDs*. The ECHR decision- which expanded the context of the right to one's image - is stressed: the right to control the use of one's image "also covers the individual's right to object to the recording, conservation and reproduction of the image by another person".[66] According to the regulation of the Civil Code of the Republic of Lithuania, a photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his/her consent. However, the consent shall not be required if such acts are related to a person's public activities, his official post, request of law enforcement agencies, or where a person is photographed in public places, but are not allowed to be demonstrated, reproduced, or sold only if those acts were to abase person's honour, dignity or damage his professional reputation.[67] However, even if a person is being photographed (filmed) in a public place, but shows clear disagreement with that, such filming should be discontinued, as the person in public places does not lose the protection of his/her privacy. The consent of being photographed could be given either verbally or in writing or even through conclusive actions, and in each particular case the limits of the consent are important as the consent to take photographs *ex officio* does not imply the consent in any way to reproduce, sell, display, print the photo.[68]

The following section (3.2) covers relevant aspects of "home" (as a value falling within the scope of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms). The Lithuanian legislator has taken a "safe" position in case there is unclear whether particular premises are treated as home or not. When the offence could not be treated as a trespass under Article 165 of the Criminal Code of the Republic of Lithuania, the injured person can always exercise his right to judicial protection under the norm of the Civil Code of the Republic of Lithuania which enshrines civil liability for "unlawful invasion of person's dwelling or other premises".[69]

---

[66] *Reklos and Davourlis v. Greece*, no. 1234/05, § 40, 15 January 2009.

[67] Civil Code of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos civilinis kodeksas), 18.07.2000 Lithuania, Official Gazette (2000), No. 74-2262; 200, Article 2.22.

[68] *T. G. v. R. Š., UAB "X"*, the decision of the Supreme Court of Lithuania of 24.02.2003, case No. *3K-3-294/2003*; *S. Š.* ir *V. Š.* v. *UAB "X"*, the decision of Supreme Court of Lithuania of 02.01.2008, case No. 3K-7-2/2008.

[69] Civil Code of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos civilinis kodeksas), 18.07.2000 Lithuania, Official Gazette (2000), No. 74-2262; 200, Article 2.23 part 2; Meškauskaitė, L., Lankauskas, M. (2016). Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos Žmogaus Teisių Teismo bei Lietuvos

Section 3.3 undertakes an analysis of the "household exemption" enshrined in the *GDPR*. The provisions of *GDPR* presuppose an idea that personal or household activities undertake any relationship that is not connected with professional or commercial activities,[70] therefore personal data processing in such a relationship is not governed by *GDPR*.[71] However, surveillance by CCTV cameras of a residential territory, at least partially covering a public street, does not fall under the "household exemption" which means that *GDPR* applies and proves that the application of this exemption is not as simple as it may seem from the provisions of *GDPR*. Many other aspects that have to be taken into consideration when deciding whether the exemption applies in the relationship when visual information recording is carried on, are illustrated by a scheme suggested by the author of the research, which requires answering a chain of questions: who the visual information recording is carried on by (legal or natural person), for what purposes, is the video record stored, is private territory regularly entered by persons having no personal relationship with the data processor

The 4th chapter: "Problematic aspects of national regulation related to privacy protection in the use of VIRDs and the possible remedies". In the sub-chapter 4.1, the author justifies the chosen research strategy and explains that there are very few cases related to privacy breaches in the use of *VIRDs* in national courts and their facts undertake only narrow, isolated issues the analysis of which would not allow to make a comprehensive analysis (maybe it is because of insufficient or inadequate regulation on the issue because of which people do not exercise their right to judicial protection). Thus, case modelling as a method allows for making logical conclusions concerning the application of privacy protection rules enshrined in the current legislation and serves for finding the solutions in the adoption of legal tools.

Sub-chapters (4.2, 4.3, and 4.4) contain three different modelled situations relating to the use of *UAS*, a photo camera in a public place and a dashboard camera respectively. The author analyses each situation in detail, trying to adapt the existing legal instruments for privacy protection. Moreover, stresses the inadequacies of the regulatory framework in the use of these *VIRDs* and suggests guidelines for its improvement.

teismų praktikos kontekste (Criminal Liability for Privacy Violations in the Context of the European Convention on Human Rights and Lithuanian Case Law). *Teisės problemos*, Vol. 1(91), p. 65.

[70] 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). Published: OJ L 119, 4.5.2016, pp. 1–88, recital point 18.

[71] 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). Published: OJ L 119, 4.5.2016, pp. 1–88, Article 2 part 2 clause c.

The problematics related to the use of *UAS* is mainly concerning the practical application of liability because of the specificity of *UASs*, which enables covert surveillance or surveillance without the identification of the responsible person. Even though the new *UAS*-related detailed legislation on the *EU* level has recently come into force, a loophole for abuse could be the exceptions of the *UAS* remote identification requirement. The two other situations are mostly related to the practical application of the right to the protection of one's image the most sensitive aspect of which is its protection in public places. These situations through the right to one's image could also be linked with certain aspects of data protection which is quite defective in Lithuania.

The 5th chapter: "Requirements for a well-balanced legislation". The final chapter is structured into four subchapters. The first three sub-chapters analyse the criteria for well-balanced legislation. The most important issue in regulation of the use of *VIRDS* is the lack of it. the non-existence of regulation on the use of dashboard cameras is unjustifiable as considering their technical characteristics, they are not much less a threat to privacy than other types of *VIRDs*. The mere knowing that dashboard cameras are always used for monitoring public places (traffic and the surroundings), their use would not formally correspond to the requirements of *GDPR* as it is not even possible to get everybody's consent for such processing. Mere this consideration proves the necessity to regulate the use of this type of *VIRD* by law and to at least ensure that individuals expecting privacy even in public places would be clearly informed about the ongoing video recording process (it could be done, for example, by requiring the users of the vehicles in which dashboard cameras are used to be marked with a special sign in precisely determined places).

Efficiency is another quality of well-balanced legislation because the longer the privacy breach lasts, the worse consequences could be caused to an individual. When Lithuanian State Data Protection Inspectorate tends to refuse to deal with complaints against natural persons, the Latvian Data State Inspectorate requires the applicant himself/herself to perform a number of actions (including correspondence with the data processor) to be established before filing a complaint to the institution.[72] Such a requirement not only prolongs the duration of the breach against an individual's privacy but also is a heavy burden on the applicant requiring even legal knowledge. The legislation is also treated as inefficient when it is outdated, in other words, not reflecting the problematics of today. In this case – not reflecting the advances in modern technology which has caused the increase of the risk to breach privacy. As examples of outdated legislation related to the use of *VRIDs* could be mentioned Lithuanian civil code which, even though enshrining the rules on privacy protection,

[72] Andersone, D. (2019). Personas datu aizsardzības krimināltiesiskie (Criminal aspects of personal data protection) (Doctoral thesis). Retrieved 02.01.2021 from aspektihttps://dspace.lu.lv/dspace/handle/7/48862.

requires the claimant to prove the respondent's fault in privacy-breach cases, whereas the unlimited possibilities of *VIRDs* cause a particularly high risk of invasion of privacy and allow carry out covert privacy data collection, the breachers to remain unidentified or to hide evidence proving the fault of the offender. The inefficiency of a piece of legislation may be due to its incompleteness or intricacy. For example, *GDPR* on the one hand is the solution of filling the gaps in privacy protection in national legislation (in cases when the personal data is processed in commercial activities), on the other hand, is so complex and comprehensive legislation[73] that, as some authors suggest, is impossible to comply with and hence ignored or discredited as conducive to abuse of rights and unreasonable.[74] An example of such uncertainty in the *GDPR* is a household exemption which is the ground for non-application of *GDPR*. Uncertainty of the "household exemption" makes it hard to apply *GDPR* against natural persons – illegal personal data collectors. So, this provision is so ambiguous that, for example, the Lithuanian State Data Protection Inspectorate got into its traps and applies this exception in all cases when a data collector is a natural person. In such a way subject of personal data loses his/her chances to defend his/her interests under *GDPR* at the national level.

Proportionality is another criterion of well-balanced legislation. However, when talking about proportionate national legislation which has to balance between human right's protection and the freedom to use another good (in this case, *VIRDs*), and presuming that there are no evident grounds for permissible interferences enshrined in Article 8 part 2 of the *Convention*,[75] in this author's opinion, the principle of proportionality should also be looked at from another point of view: whether the protection of human right is adequate and not too much restraining that other value against which the human right is sought to be balanced.

[73] Sirur, S., Nurse, J., Webb, H. (2018). Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). Conference: Proceedings of the International Workshop on Multimedia Privacy and Security (MPS) at the 25th ACM Conference on Computer and Communications Security (CCS), (available online at https://www.researchgate.net/publication/327160034_Are_We_There_Yet_Understanding_the_Challenges_Faced_in_Complying_with_the_General_Data_Protection_Regulation_GDPR), p. 1.

[74] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, Vol. 10(1), p. 41.

[75] Convention for the Protection of Human Rights and Fundamental Freedoms. Signed in Rome 04.11.1950. Latvia joined the treaty on 27.06.1997. Law "On European Convention for the Protection of Human Rights and Fundamental Freedoms 4th November 1950 and its protocol 1st, 2nd, 4th, 7th and 11th protocol." Published Latvijas Vestnesis, 143/144, 13.06.1997, Article 8 part two states: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Thus, the use of VIRDs by natural persons in most of the cases do not correspond the notion "rights and freedoms of others" and are not among those grounds permitting intereference with the exercise of the right to respect for private life, therefore has to be governed in the way as not to breach the human right.

Regulation is not proportionate when the liability applicable for the infringement does not correspond to its seriousness. For example, privacy protection for certain breaches related to personal data is not ensured by administrative law therefore directly leads to criminal proceedings. Such a situation may occur in case when personal data is processed for personal reasons (for example, a spouse is gathering evidence on infidelity for a divorce case (which, under Lithuanian case law is usually treated as permissible evidence)[76] but later the court finds that the limits of such permissibility have been exceeded. Administrative liability as a punitive and preventive legal tool could not be applicable as neither national (Latvian and Lithuanian) laws on data protection apply for such a case nor *GDPR*). Thus, for punitive and preventive reasons only criminal liability would be applicable. However, if the offender was gathering, as he/she might have thought, permissible evidence for the case, such a type of liability would be completely disproportionate.

Sub-chapter 5.4 provides for final remarks on Lithuanian and Latvian regulation of privacy protection in the use of visual information recording devices by natural persons. The main difference between Latvian and Lithuanian regulations is that the latter clearly separates privacy and data protection, whereas the former equates privacy and data protection. Such a conclusion can be drawn from the fact that the Criminal Law of the Republic of Latvia has only one general rule on the protection of privacy-related interests – personal data.[77] The regulation on the right to the protection of one's image in the Civil Code of the Republic of Lithuania is not sufficient as privacy is not protected in public places (therefore the author suggests the rule of "sole object" of the photography which would oblige the photographer to receive the consent of a person to be photographed if he/she is the sole/main object of the photography and is recognisable in it, whereas the regulation on privacy should be improved in the part of the compensatory mechanism (the author suggests enshrining strict liability in cases when the privacy breach is done by using *VIRDs* and other technologies)).

A thesis submitted for defence, conclusions, and proposals:

Summarising the results of the research, the answer to the research question of whether Lithuanian state regulation on the use of *VIRDs* is sufficient for the effective protection of privacy in this field is "no". Thus, the following conclusions and suggestions could be drawn:

1. As the application of the *EU* law in the protection of privacy in the use of *VIRDs* is inevitable, and a person's image under *ECJ* case-law constitutes personal data, provisions of *GDPR* are of particular importance. However, this *EU* legislation is quite complicated, especially when

[76] *A. Š v. J. Š*, the ruling of the Supreme Court of Lithuania of 06.06.2012, case No. 3K-3-269/2012.
[77] Criminal Law (Krimināllikums). Adopted on 17.06.1998. Published: Latvijas Vēstnesis, 199/200, 08.07.1998; Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 15, 04.08.1998. Last amendments 11.06.2020, Article 145.

talking about "household exemption". Lithuanian Supervisory authority applies for this exemption incorrectly by presuming that if the data processor is not a legal person, "household exemption" applies and refuses to investigate the case. Such interpretation is faulty because the person whose legitimate interests have been breached cannot defend his/her interests against such offender using administrative tools: the provision on personal data breach in the Code of Administrative Offences has been repealed as redundant because the liability is governed by *GDPR*, but *GDPR* is not applicable either. This leads to a situation when data subject's right to the protection of privacy, personal data may be protected by civil proceedings only, which is a long-lasting process and therefore may be ineffective.

In order to avoid such a situation, the author of the research suggests national supervisory authority or other institutions (their officials) dealing with complaints concerning personal data breaches in cases of visual information recording, apply a test, which requires to answer a chain of questions and leads to the corresponding answer ("household exemption" applies, *GDPR* applies, the matter is not governed by *GDPR*).

2. Civil proceedings in the protection of privacy in Lithuania are not effective not only because they are long-lasting (this applies in cases when the claimant seeks for urgent termination of the infringement of his privacy) but also because, firstly, the claimant bears the excessive burden of proof (he/she is required to prove fault of the respondent), secondly, the compensation for non-pecuniary damage awarded by Lithuanian courts is usually too small to achieve its purposes (to compensate for negative consequences of the infringement), thirdly, the courts sometimes do not award non-pecuniary damage reasoning that the mere fact of the recognition of the privacy breach is satisfactory enough to compensate the non-pecuniary damage, fourthly, the courts in some cases interpret the type of fault as the measure allowing not to decide the amount of non-pecuniary damage to be awarded but as the criteria allowing to determine the merits of the claim for non-pecuniary damage (in other words, if an intentional fault is not proven by the claimant, the courts treat that the compensation for non-pecuniary damage should not be awarded).

Taking into consideration the importance of an image as an information source, and the fact that Article 6.248 of the Civil Code indicates that civil liability arises without fault in the cases established by law, it is suggested to supplement Book six, Part three, Chapter XXII, Section three of the Civil Code of the Republic of Lithuania with an additional article: "Liability for invasion of privacy committed through the use of visual information recording devices" which should state that "If privacy has been breached through the use of visual information recording devices, the guilty party

shall be liable to compensation for the damage," in such a way enshrining strict liability which would not require the claimant to prove the respondent's fault.

The following recommendations are addressed to the courts of Lithuania: it is recommended to the courts in their practice to avoid using the type of fault as the criteria allowing to determine whether claimant's request to award non-pecuniary damage is substantiated and should be satisfied, as any privacy breach, despite the type of fault of the violator, causes non-pecuniary damage, it is only a question of its amount. Furthermore, in this author's opinion, the mere fact of recognition of the violation, should not be treated as sufficient compensation for non-pecuniary damage because it does not add any value to the privacy protection mechanism. Finally, the courts should avoid awarding symbolic compensations for non-pecuniary damage as it discourages privacy subjects to defend their violated privacy in courts.

3. Privacy in the field of the use of *UASs* is properly protected neither at the *EU* level nor at the national level. *Regulations 2019/947* and *2019/945* do not ensure identification of the *UAS* operator (pilot) when the *UAS* being used is classified in class C0 and C4 or it is treated as a toy in the meaning of Directive 2009/48/EC on the safety of toys. As identification of the pilot (operator) is an essential condition for tackling possible privacy breaches, also their prevention, exceptions to the requirement to be equipped with remote identification add-ons allowing the competent authority from the distance to identify the position of the remote pilot, determine his/her identity, height above the surface, the take-off point is the area for abuse. Furthermore, *Regulation 2019/947* does not speak about effective measures in terminating the infringement in real-time (when the *UAS* is being in operation). Even though *Regulation 2019/947* allows Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of Regulation (EU) 2018/1139, including protection of privacy and personal data in accordance with the Union law, Lithuania, in its national rules simply transposed provisions or the *Regulations 2019/947* and *2019/945* but has not adopted any specific rules serving for protection of privacy.

Considering the shortcomings in the *Regulations 2019/947* and *2019/945* serving for possible privacy violators and exercising its right to lay down national rules specifying the *Regulation 2019/947* and serving for privacy protection, Lithuania should adopt special rules on the operation of *UASs* and to lay down provisions helping effectively ensure privacy protection, such as: flight restrictions in terms of time and territory (taking Latvian example, to enshrine flight ban between 30 minutes after sunset and until 30 minutes before sunrise), the requirement not to fly *UASs* closer than 2 meters in the horizontal plane from the street edge of populated areas (towns and villages or detached residences)). Also, it is suggested that a remote pilot, operating *UAS* which is not required under *EU*

regulation to be equipped with remote identification add-on, during the operation of such *UAS* was easily identifiable (for example, should be obliged to wear bright west with a drone sign) and stay in a visible line from the *UAS* being in operation (an exception to the latter requirement could be made only for *UASs* of class C4 in sports events). The same law should empower the competent authority to preserve evidence in suspected privacy breaches (because in order to apply criminal liability for privacy (personal data) breaches in Lithuania, it is required to prove direct intent to commit a crime). Also, the national authority should be empowered to neutralise *UAS* if precise, clear conditions are satisfied (for example, if the identification of *UAS* pilot or operator is impossible and there is a verbal or written claim against the operator for suspected breach of privacy).

4. When Latvian Personal Data Processing Law enshrined prohibition to disclose records obtained in road traffic to other persons and institutions (except for separately indicated cases), the use of dashboard cameras is not regulated by any specific rules in Lithuania. The problematics with the use of dashboard cameras unfold in two aspects. The first aspect, when the camera takes records of the inside of a car. In such a case it is important whether the inside of the car is treated as a public or non-public place. Depending on the latter, different legal tools to protect privacy-related interests are applied. If the inside of a car is treated as a private place, privacy protection rules shall apply, whereas if not – personal data protection rules could be invoked. The second aspect is related to a situation when a dashboard camera takes records of the outside of the car. The non-existence of the regulation on the use of dashboard cameras in Lithuania makes the use of such devices unregulated or even illegal in the context of *GDPR*, because there are no exceptions to their use in this legislation and in the national laws, whereas the use of dashboard cameras could definitely be treated as personal data processing (because the public area is being observed, personal data is being processed (for example, car registration numbers)), dashboard camera is treated as automated mean under Article 2 part 1 of *GDPR* and "household exemption" does not apply. If under the case-law of *ECJ* using *CCTV* camera recording covers, even partially, a public space processing the data in that manner cannot be regarded as an activity which is a purely 'personal or household' activity and *GDPR* applies, it is not understandable, why dashboard cameras should be treated differently.

As the use of this type of *VIRD* is undeniable, therefore there must be found a way of balancing dashboard camera use with privacy protection. Considering the fact that currently there is no special regulation on the use of such a device, Lithuanian legislation, for example, Law on Personal Data Legal Protection, taking Latvian example, could be supplemented by an article stating that "If automated data recording equipment is used in road traffic for personal or household use, the requirements of this law, as well as *GDPR*, do not apply. Records obtained in road traffic cannot be

disclosed to other persons and institutions (except for separately indicated cases).” Alongside it is necessary to enshrine special marking of the vehicles in which dashboard cameras are used (for example, placing the sign on all sides of the car so that it is easily visible in road traffic), in such a way alerting other road users to the ongoing video capture. Besides personal data protection, such marking would serve for the investigation of road traffic accidents, when video records are necessary to investigate the circumstances of road accidents).

5. Lithuanian legislation, namely Article 2.22 of the Civil Code of the Republic of Lithuania, separately governs the protection of the right to one’s image. This article makes processing personal data (precisely, an image) lawful in public places without the data subject’s consent, unless such processing was to abase a person’s honour, dignity, or damage his professional reputation. On the one hand, this article could be understood as derogation for *GDPR* for the purpose of balancing personal data protection and freedom of expression. On the other hand, such regulation does not correspond with *ECHR* case law which has confirmed that the protection of an image begins before the photo is taken and that individuals do not lose their privacy even in a public place. Current regulation enshrined in the just-mentioned article of the Civil Code means that if the photo was taken in a public, the protection of personal data is less than the one enshrined in *GDPR*. Thus, if the processing of an individual’s personal data does not infringe his/her honour, dignity (i.e. privacy), this person does not have legal grounds to prove that such processing is unlawful and the respondent in a civil case (data processor) would not even have to prove that the conditions of freedom of expression existed at the moment the photo was taken – such processing would automatically be lawful because of the mere fact that the photo was taken in a public place.

Such regulation of the protection of an image is faulty. Taking into consideration Article 2.22 of the Civil Code of the Republic of Lithuania, which states that “Photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his consent. Such consent after natural person’s death may be given by his spouse, parents or children”, the second part of this article (which currently sounds: “Where such acts are related to person’s public activities, his official post, request of law enforcement agencies or where a person is photographed in public places, consent of a person shall not be required. Person’s photograph (or its part) produced under the said circumstances, however, may not be demonstrated, reproduced or sold if those acts were to abase person’s honour, dignity or damage his professional reputation”), should be adjusted as follows: “If a natural person is the sole or one of the main objects of the camera of the visual information recording device and that natural person could be identified from the photo/video to be made, the person may be photographed only with his/her consent.

Derogation from this rule is allowed only if the right of freedom of expression and information is exercised."

6. Technological achievements and social processes cannot be suppressed in order to fit the existing laws that do not match reality anymore, therefore the evolutionary gap between technical progress and legal implementation rules has to be filled. Thus, the specific characteristics of visual information recording devices making them more threatening to privacy (such as the possibility of secret surveillance, image recording, or mobility) require special regulation. However, the regulation cannot be too restraining technological development and use because modern technologies have a non-exhaustive list of benefits, including life-saving and economic ones. For these reasons, the regulation has to meet the criteria of effectiveness, efficiency, and proportionality and this would be done if the above-mentioned proposals were implemented.

The main scientific literature sources used in the thesis:

1. Abulashvili, V. (2018). Human Rights and Development of Technology. *L'Europe Unie/United Europe*, Vol. 12/2018, pp. 47-54.

2. Akandji-Kombe, J. F. (2007). Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights. *Human rights handbooks*, Vol. 7, pp. 1-72.

3. Andersone, D. (2018). Personas datu aizsardzības krimināltiesiskie (Criminal aspects of personal data protection) (Doctoral thesis). Retrieved 02.01.2021 from aspektihttps://dspace.lu.lv/dspace/handle/7/48862.

4. Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level (2018). Retrieved 15.12.2019 from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_en.pdf. doi:10.2811/06311

5. Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. Retrieved 24.06.2018 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

6. Bakircioglu, O. (2007). The Application of the Margin of Appreciation Doctrine in Freedom of Expression and Public Morality Cases. *German Law Journal*, Vol. 08(7), pp. 711-734. doi: 10.1017/S2071832200005885

7. Banisar, D., Davies, S. (1999). Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *Journal of Computer & Information Law*, Vol. XVIII, pp. 1-112.

8. Brunk, B. (2002). Understanding the privacy space. *First Monday*, Vol. 7(10) (online journal available at: https://firstmonday.org/ojs/index.php/fm/article/view/991/912).

9. Bučiūnas, G. (2015). Vaizdo registratoriai ir asmens privatumas. *Mokslo taikomieji tyrimai Lietuvos kolegijose*, Vol. 1(11), pp. 64-68.

10. Cayford, M., Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, Vol. 34(2), pp. 88-103. doi: 10.1080/01972243.2017.1414721. doi: 10.1080/01972243.2017.1414721

11. Cannataci, J.A. (2010). Squaring the Circle of Smart Surveillance and Privacy. *Fourth International Conference on the Digital Society*, pp. 323-328. doi: 10.1109/ICDS.2010.55

12. Cirtautienė, S. (2013). Impact of Human Rights on Private Law in Lithuania and other European Countries: Problematic Aspects. *Jurisprudence*, Vol. 20(1), pp. 77-90.

13. Council of Europe. The Margin of Appreciation. Retrieved 29.07.2019 from https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp.

14. Diggelmann, O., Cleis, M. N. (2014). How the Right to Privacy Became a Human Right. *Human Rights Law Review*, Vol. 14, 441–458. doi: 10.1093/hrlr/ngu014

15. Dolzhikov, A. V. (2012). The European Court of Human Rights on the Principle of Proportionality in "Russian" cases. *Teisė*, Vol. 82, pp. 215-224. doi: 10.15388/Teise.2012.0.127

16. Dupate, K. (2011). Case Law of the Court of Justice of the European Union (Eiropas Savienības Tiesas Prakse Darba Tiesībās). Retrieved 27.04.2020 from https://arodbiedribas.lv/wp-content/uploads/2019/11/es_tiesas_prakse_darba_tiesibas.pdf.

17. ECHR Research Division (2013). National security and European Case-Law. Retrieved 01.08.2019 from https://rm.coe.int/168067d214.

18. EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019). Retrieved 27.03.2020 from https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

19. European Commission, "Communication for the Commission to the European Parliament and the Council, A New Era for Aviation. Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner" (2014). Retrieved 01.07.2019 from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0207&from=EN.

20. European Data Protection Board (2019). Guidelines 3/2019 on processing of personal data through video devices. Retrieved 2020.01.03 from https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

21. European Data Protection Board (2020). Guidelines 3/2019 on processing of personal data through video devices. Retrieved 02.15.2020 from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.

22. European Parliament (2007). Explanations relating to the Charter of Fundamental Rights of the European Union, OJ C 303, 14.12.2007, p. 17–35.

23. European Parliamentary Research Service (October 2018). The right to Respect for Private Life: Digital Challenges, a comparative law perspective. Retrieved 01.02.2020 from https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628249/EPRS_STU(2018)628249_EN.pdf. doi:10.2861/45028

24. European Union Aviation Safety Agency (2019, 9 October). Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947. Retrieved 12.12.2019 from https://www.easa.europa.eu/sites/default/files/dfu/AMC%20%26%20GM%20to%20Commission%20Implementing%20Regulation%20%28EU%29%202019-947%20%E2%80%94%20Issue%201.pdf.

25. Florijn, A. N. (2008). Quality of legislation: A law and development project. *Explorations in theory and practice of international legislative projects: Lawmaking for development*. Leiden University Press, pp. 75-89.

26. Goldstein, K., Ohad, S., Tov, M., Prazeres (2018). The Right to Privacy in the Digital Age, available at https://www.researchgate.net/publication/328789396_The_Right_to_Privacy_in_the_Digital_Age.

27. Greer, S. (1997). *The exceptions to articles 8 and 11 of the European Convention on Human Rights*. Human rights files No. 15. Council of Europe Publishing, 67 p. ISBN 978-92-871-3373-1

28. Greer, S. (2000). *The Margin of Appreciation: Interpretation and Discretion Under the European Convention on Human Rights.* Human rights file No. 17. Council of Europe Publishing, 60 p. ISBN: 9287143501

29. Griffin, J. (2007). The Human Right to Privacy. *San Diego Law Review*, Vol. 44(4), pp. 697-722.

30. Guide on Article 8 of the European Convention on Human Rights, retrieved at 03.01.2020 from https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

31. Hert, P. (2005). Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11. *Utrecht Law Review*, Vol. 1(1), pp. 68-96. doi: 10.18352/ulr.4

32. Hoofnagle, C. J., Sloot, B., Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, Vol. 28(1), pp. 65-98. doi: 10.1080/13600834.2019.1573501

33. Hughes, K. (2019). The Public Figure Doctrine and the Right to Privacy. *Cambridge Law Journal*, Vol. 78(1), pp. 70-99. doi: 10.1017/S000819731900028X

34. Human Rights Council of the United Nation (2020). Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights (advance edited version), retrieved 14.02.2021 from https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf.

35. Jarašiūnas, E. (2017). European Union Charter of Fundamental Rights in the Case-law of the Court of Justice. *Jurisprudence*, Vol. 24(1), pp. 6-34.

36. Jočienė, D., Čilinskas, K. (2004). *Žmogaus teisių apsaugos problemos tarptautinėje ir Lietuvos Respublikos teisėje* (*Problems of Human Rights Protection in International and Lithuanian Law*). Vilnius, UAB "Petro ofsetas", 232 p. ISBN: 9955534576

37. Katuoka, S. (2013). Europos Sąjungos teisės ir tarptautinės teisės santykio klausimu (On the Relationship of the European Union and International Law). *Jurisprudencija*, Vol. 20(3), pp. 841–854. doi: 10.13165/JUR-13-20-3-02

38. Kavalnė, S., Danėlienė, I. (2016). The European Union Charter of Fundamental Rights as an instrument of protection of individual rights. *Jurisprudencija*, Vol. 22(2), pp. 231-251. doi: 10.13165/JUR-15-22-2-03

39. Kilkelly, U. (2003). The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights. *Human Rights Handbooks Series*, Vol., p. 72. Retrieved 01.17.2016 from https://rm.coe.int/168007ff47.

40. Kokott, J., Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, Vol. 3(4), pp. 222-228. doi: 10.1093/idpl/ipt017

41. Korff, D. (2009). The Standard Approach to Case Assessment Under Articles 8-11 and Article 2 ECHR. Retrieved 22.07.2019 from

http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf.

42. Krishnamurthy, V. (2020). A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *AJIL Unbound*, Vol. 114, pp. 26-30. doi: 10.1017/aju.2019.79

43. Krūma, K., Statkus, S. (2019). *The Constitution of Latvia – A Bridge Between Traditions and Modernity. National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*. T.M.C. Asser Press, The Hague, pp. 951-995. doi: 10.1007/978-94-6265-273-6_20

44. Kuhn, Z. (2018). The Ryneš case and liability for invasion of privacy in the 21st century. *CYELP*, Vol. 14, pp. 241-253. doi: 10.3935/cyelp.14.2018.302

45. Lankauskas, M. (2007). Balancing the Right to privacy from the Freedom of expression according to the jurisprudence of the European Court of Human Rights. *Teisės problemos*, Vol. 2 (56), pp. 103-131.

46. Lauren, P. G. (2011). *The Evolution of International Human Rights: Visions Seen (3rd edn.)*. Pennsylvania: University of Pennsylvania Press, 414 p. doi: 10.9783/9780812209914

47. Li, H., Yu, L., He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, Vol. 22(1), pp. 1-6. doi: 10.1080/1097198X.2019.1569186

48. Lidsky, L. B. (1998). Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It. *Tulane Law Review*, Vol. 73, pp. 418-421.

49. McKown, M. (2015). The New Drone State: Suggestions for Legislatures Seeking to Limit Drone Surveillance by Government and Nongovernment Controllers. *University of Florida Journal of Law and Public Policy*, Vol. 26, pp. 71–90.

50. Merrills, J. G., Robertson, A. A (2001). *Human Rights in Europe: Study of the European Convention on Human Rights (4th edn.).* Manchester: Manchester University Press, 362 p.

51. Meškauskaitė, L. (2015). *Teisė į privatų gyvenimą*. Vilnius: VĮ "Registrų centras", 336 p. ISBN: 9789955301783

52. Meškauskaitė, L. (2005). Žiniasklaidos pažeistų asmens konstitucinių teisių gynimo būdai. *Jurisprudencija*, Vol. 64, pp. 114-123.

53. Mikelsone, G. (2013). The Binding Force of the Case Law of the Court of Justice of the European Union. *Jurisprudence*, Vol. 20(2), pp. 469-495. doi: 10.13165/JUR-13-20-2-06

54. Misiūnaitė-Kamarauskienė, D. (2014). Recent case-law of the Court of Justice of the European Union regarding the fundamental rights to respect for private and family life and to

protection of personal data. *Jurisprudence*, Vol. 21(4), pp. 1233-1245. doi: 10.13165/JUR-14-21-4-15

55. Mollers, N., Halterlein, J. (2013). Privacy issues in public discourse: the case of "smart" CCTV in Germany Innovation. *The European Journal of Social Science Research*, Vol. 26(1-2), pp. 57-70. doi: 10.1080/13511610.2013.723396

56. Moreham, N. A (2005). Privacy in the Common Law: A Doctrinal and Theoretical Analysis. *Law Quarterly Review*, Vol. 121, pp. 628-656.

57. Moreham, N. A. (2006). Privacy in Public Places. Victoria University of Wellington Legal Research Paper No. 111/2015. *Cambridge Law Journal*, Vol. 65, pp. 606-635.

58. Moreham, N. A. (2008). The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination. *European Human Rights Law Review*, Vol. 1, pp. 44-80.

59. Murdoch, J., Roche, R. (2013). The European Convention on Human Rights and policing. Retrieved 03.01.2020 from https://www.echr.coe.int/Documents/Handbook_European_Convention_Police_ENG.pdf.

60. Nelson, J. R., Grubesic, T. H., Wallace, D., Chamberlain, A. W. (2019). The View from Above: A Survey of the Public's Perception of Unmanned Aerial Vehicles and Privacy. *Journal of Urban Technology*, Vol. 26(1), pp. 83-105. doi: 10.1080/10630732.2018.1551106

61. Norkūnas, A. (2002). Kaltė kaip civilinės atsakomybės pagrindas. *Jurisprudencija*, Vol. 28(20), pp. 112-118.Pfisterer, V. M. (2019). The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy. *German Law Journal*, Vol. 20, pp. 722–733. doi: 10.1017/glj.2019.57

62. Pūraitė, A., Bereikienė, D., Šilinskė, N. (2017). Regulation of unmanned aerial systems and related privacy issues in Lithuania. *Baltic Journal of Law & Politics*, Vol. 10:2, pp. 107-132. doi: 10.1515/bjlp-2017-0014

63. Pūraitė, A., Šilinskė, N. (2019). Image capturing devices: threat or good. *Problems of Legality*, Vol. 144, pp. 120-137. doi: 10.21564/2414-990x.144.157226

64. Pūraitė, A., Šilinskė, N. (2020). Privacy protection in the new EU regulations on the use of unmanned aerial systems. *Visuomenės saugumas ir viešoji tvarka*, Vol. 24, pp. 173-183. doi: 10.13165/PSPO-20-24-11

65. Pūraitė, A., Šilinskė, N. (2021). State regulation of privacy and its protection in the use of VIRDs by police: comparative perspective from Latvia and Lithuania. *Visuomenės saugumas ir viešoji tvarka*, Vol. 27, pp. 115-132. doi: 10.13165/PSPO-21-26-32

66. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, Vol. 10(1), pp. 40-81. doi: 10.1080/17579961.2018.1452176

67. Roagna, I. (2012). Protecting the right to respect for private and family life under the European Convention on Human Rights. *Council of Europe human rights handbooks*. Retrieved 05.06.2017 from https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf .

68. Rogavichene, L., Garmonnikov, I. (2017). Innovative Technologies for Assessment and Correction of the Driving Style. *Transportation Research Procedia*, Vol. 20, pp. 564-570. doi: 10.1016/j.trpro.2017.01.091

69. Schauer, F. (1998). Internet Privacy and the Public-Private Distinction. *Jurimetrics*, Vol 38(4), pp. 555-564.

70. SESAR (2017). European Drones Outlook Study. Retrieved 01.02.2018 from https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf.

71. Smith, A. T. H., Moreham, N., A. (2019). Privacy – Police Photographs in Public Places. *Victoria University of Wellington Legal Research Papers*, Vol. 9(3), pp. 20-22.

72. Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, Vol. 90, pp. 1087-1155. doi: 10.2307/3481326

73. Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Vol. 154(3), pp. 477-560.

74. Solove, D. J. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press, 24 p. ISBN-10: 0-674-02772-8

75. Stepanovic, I. (2014). Modern Technology and Challenges to the Protection of the Right to Privacy, *Belgrade Law Review*, Vol. 3, pp. 167-178. doi: 10.5937/AnaliPFB1403167S

76. Torgans, K., Karklinš, J. and Bitans, A. (2017). *Ligumu Un Deliktu Problemas Eiropas Savieniba un Latvija* (Contract and Tort Problems in the European Union and Latvia). Riga: Tiesu namu agentūra, pp. 414.

77. UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988. Retrieved 27.07.2019 from https://www.refworld.org/docid/453883f922.html.

78. United Nations, The Foundation of International Human Rights Law. Retrieved 06.07.2019 from https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html.

79. Vacek, J.J. (2014). Remote Sensing of Private Data by Drones is Mostly Unregulated: Reasonable Expectations of Privacy Are at Risk Absent Comprehensive Federal Legislation. *North Dakota Law Review*, Vol. 90, pp. 463-484.

80. Vermeulen, M. (2014). Surveille. Deliverable D4.7 The scope of the right to private life in public places. Retrieved 14.11.2017 from https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.7-The-scope-of-the-right-to-privacy-in-public-places.pdf.

81. Villasenor, J. (2013). Observations from Above: Unmanned Aircraft Systems and Privacy.*Harvard Journal of Law & Public Policy* 36, pp. 457-517.

82. Warren, S. D., Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4(5), p. 193-220. doi: 10.2307/1321160

83. Weeramantry, C. G. (1993). *The impact of technology on human rights: global case-studies*, New York: United Nations University Press, introduction in online version (available at https://archive.unu.edu/unupress/unupbooks/uu08ie/uu08ie00.htm#Contents). ISBN: 92-808-0821-4

84. Wilton, R. (2017). After Snowden – the evolving landscape of privacy and technology. *Journal of Information, Communication and Ethics in Society*, Vol. 15(3), pp. 328-335. doi: 10.1108/jices-02-2017-0010

85. Ziegler, K. (2016). The Relationship between EU Law and International Law. *A Companion to European Union Law and International Law*, New York, United States: John Wiley & Sons Inc, pp. 42-61. doi: 10.1002/9781119037712.ch4

Author: Neringa Šilinskė _____ 2021