ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2021 (27)

STATE REGULATION OF PRIVACY AND ITS PROTECTION IN THE USE OF VIRDS BY POLICE: COMPARATIVE PERSPECTIVE FROM LATVIA AND LITHUANIA

Aurelija PŪRAITĖ
Mykolas Romeris University
Maironio str. 27, LT 44211 Kaunas, Lithuania
E-mail: aurelija.puraite@mruni.eu
ORCID ID: 0000-0001-9228-1396

Neringa ŠILINSKĖ
Turiba University
Zemgale Suburb, Riga, LV-1058, Latvia
E-mail: n.silinske@gmail.com
ORCID ID: 0000-0001-7758-8883

DOI: 10.13165/PSPO-21-26-32

Abstract. *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). This research is focused on use of VIRDs by police in Latvia and Lithuania – legal regulation in both countries and its disfunctions, however, the research includes only general aspects of privacy protection in the use of VIRDs by a Public Police (except for their use against outside threats) as the most directly and extensively touching individuals' privacy aspects, because such use is widespread, relevant to most of the people as it is used in the everyday practice of the Public Police in public places. It is necessary to systematically investigate how privacy protection is ensured in particular national jurisdictions 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. VIRD in this 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).*

Keywords: *privacy protection, state regulation in Latvia and Lithuania, visual information recording devices*

Introduction

In the constantly changing and developing world the concept of modern technologies is escalated more often. But together with the improvement of the technologies, peoples' concern about their privacy grows, therefore people have become more conscious about their fundamental rights. After a longevous and hard work of various international and national human rights institutions, people of civilized countries believe that human rights are and can be effectively defended by various legal instruments. This could be illustrated by the increasing number of cases in the European Court of Human Rights (European Court of Human Rights, 2010). However, 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. Socio-legal positivism theory accepts the Social Fact Thesis which asserts that the content of law is manufactured according to social processes (Himma, 2004, p. 217). 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" (*Von Hannover v. Germany*, 2012), "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" (*Eerikäinen and Others v. Finland*, 2009). Such importance of an image is affirmed by national courts (*Douglas v. Hello!, 2005*). 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" (Solove, 2009, p. 2) and "there appears to be [a] worldwide consensus about the importance of privacy and the need for its protection" (Pranevičienė, 2011, p. 1613), 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) (Nesterova, 2020, p. 2), 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, as Campbel (2019) indicates, Chongqing, a city in China, has one CCTV camera for every 5.9 citizens—or 30 times their prevalence in Washington, D.C. (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).

For this reason, it is necessary to systematically investigate how privacy protection is ensured in particular national jurisdictions 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. VIRD in this 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). 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.

As the problem raised in this 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. The research goal is to determine dysfunctions of Lithuanian and Latvian regulation of privacy protection in the use of VIRDs by public police.

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). This research is focused on use of VIRDs by police in Latvia and Lithuania – legal regulation in both countries and its disfunctions, however, the research includes only general aspects of privacy protection in the use of VIRDs by a Public Police (except for their use against outside threats) as the most directly and extensively touching individuals' privacy aspects, because such use is widespread, relevant to most of the people as it is used in the everyday practice of the Public Police in public places.

Privacy in the context of the use of VIRDs in Lithuanian domestic law and case-law

By national legislation, the right to privacy is protected at the national level. In Lithuanian legislation, the right to privacy is described in various legal acts the main of which is the Constitution. Its Article 22 enshrines people's right to privacy by stressing the inviolability of an individual's private life, determining that collection of information concerning the private life of an individual is allowed only upon justified court order and in accordance with the law, also enshrining the duty of the court and the law to protect individuals from arbitrary or unlawful interference in their private life (Official Gazette, 1992). Constitutional Court of the Republic of Lithuania has stated that the abovementioned provisions of Article 22 are one of the most important guarantees of inviolability of an individual's private life as his/her private life is protected not only from unlawful interference of the State, other institutions and their officials but also from the unlawful interference from other individuals (The ruling of the Constitutional Court of the Republic of Lithuania of September 19, 2002). In the same case the Constitutional Court also stressed that the limitations on the constitutional rights and freedoms, including protection of private life, are allowed only if it is done by law, they are necessary in a democratic society in an attempt to protect the rights and freedoms of others and the values and objectives enshrined in the Constitution, also if the limitations do not deny the nature and essence of the rights and freedoms and the principle of proportionality is followed. It is clear from the constitutional regulation of the principle of inviolability of private life that, in order to ensure effective protection of privacy, the process of gathering information about a person's private life is essentially formalised, associated with the procedure established by law and adoption of a court decision. Thus, it could be concluded that freely acting private persons are generally not entitled to collect such information (Supreme Court of Lithuania, 2013).

Another law connected with a particular aspect of privacy protection is the Law on Personal Data Legal Protection of the Republic of Lithuania (hereinafter – LPDLP) which is in accordance with the GDPR and protects personal information but also does not apply to the processing of personal data by a natural person with no connection to a professional or commercial activity (Official Gazette, 2000). As the national legislation must correspond to the European Union legislation, the LPDLP was changed just after the GDPR came into force so that it corresponded with the Regulation. In its previous version video surveillance, as the most helpful tool to gather private information and at the same time the most threatening privacy, was regulated by a separate article, and its limitations were set. However, after the newest changes, the article connected with video surveillance has been repealed.

Lithuania does not have any specific regulation concerning the use of any of VIRDs. The rules governing the use of UASs, which is called "The rules for the use of unmanned aircrafts" (TAR, 2014), have been repealed since 01.01.2021 because of the new regulation at the EU level. The so expected regulation at the EU level was indispensable as national (Lithuanian) regulation in this field was for assurance of physical safety only and had nothing to do with

privacy protection. Trying to find a hint about the protection of privacy in the Rules failed, as they were intended to set only physical safety requirements for the use of UASs (Puraite, Bereikiene and Silinske, 2017, p. 118).

At the time when the earlier-mentioned Regulation 2019/947 was in force, the Rules were still valid and not even amended till 01.01.2021 when the act was repealed. At the time of this research, there have been issued only by-laws on the marketing of unmanned aircraft systems (TAR, 2020a), and by-laws related to the issuance of certificates for UASs operators of various categories repeating and implementing the relevant rules set in Regulation 2019/947 (TAR, 2020b; TAR, 2020c). However, on the contrary to its neighbour Latvia, Lithuania has not yet adopted any specific rules on the flights of UASs that would complement privacy protection rules set in Regulation 2019/947.

The civil Code of the Republic of Lithuania establishes the inviolability of the individual's privacy and stresses that a person's private life may be made public only with that person's consent (Official Gazette, 2000). The following point of the same article concretizes what a violation of a person's private life is and lists actions, such as the unlawful invasion of a person's dwelling or other premises as well as fenced private territory, observation of one's private life, unlawful search of the person or his property, intentional interception of person's telephone, post or other private communications, violation of the confidentiality of personal notes and information, publication of the data on the state of his health in violation of the procedure prescribed by the laws; and states that the given list is not finite.

The regulation of the Civil code is special because the rules on privacy protection, set in it, on the contrary to the earlier mentioned LPDLP, apply also to natural persons and they enable the party whose legitimate interests have been violated, to take legal remedies, including requesting for the non-pecuniary damage. However, the following four conditions must be proved in order to apply civil liability: 1) unlawful actions; 2) causation; 3) fault; 4) damage. Breach of Article 2.23 of the Civil Code of the Republic of Lithuania or any other legal act guaranteeing the right to privacy is treated as unlawful actions. Article 6.246 of the Civil Code states that the civil liability shall arise from non-performance of a duty established by laws <...> or from performance of actions that are prohibited by laws <...>, or from violation of the general duty to behave with care.

Protection of privacy is enshrined in Lithuanian administrative and criminal law. However, the Code of administrative offences sets the fines only for unauthorized processing of personal data and privacy breaches in the area of electronic communications (applied for activities of entities, providing or entitled to provide a public communications network or related facilities only). However, the code also sets the prohibition to breach the rules on the use of unmanned aircraft, including use of unregistered, or without identification marks, aircraft, also the operation of aircraft without a valid certificate of airworthiness (except for aircraft performing test flights in the prescribed manner), use of aircraft with knowledge of non-compliance with airworthiness requirements (TAR, 2015) (Article 393, parts 2 and 6). So, this administrative tool could be used to defend the interests of privacy subjects (if noticed that the UAS is being flown over private area and requirements of distance, location, marking, etc. are breached, the injured person on the grounds of the rules on the operation of aircraft could request for stopping the UAS monitoring activities).

Section XXIV of the Criminal Code of the Republic of Lithuania sets the crimes related to the inviolability of private life. Among the crimes mentioned, there are articles criminalizing trespass (Article 165), illegal collection of information about a person's private life (Article 167), and making available to the public, exploitation, or exploitation for the benefit of third parties information about someone's private life without his consent if this information was

received for the accused person's service, profession or during the performance of a temporary task, or by committing one of the crimes named above (Article 168). However, because none of these crimes is classified as the crime for a negligent commitment of which the prosecution is allowed, and because the crimes are of formal nature (it means that for a criminal liability it is enough to commit action (inaction) outlined in the disposition of the article and negative consequences are not required)[11] in order to arraign on earlier mentioned crime charges, direct intent to commit a crime must be proven, as it is stated in Article 16 part 4 of the Criminal Code of the Republic of Lithuania: "A person shall be punishable for the commission of a crime or misdemeanour through negligence solely in the cases provided for separately in the Special Part of this Code. The same rule is confirmed in *S.B., V.B., R.B* case (Klaipeda District Court, 2011). A crime or misdemeanour is treated as committed with a direct intent where: 1) when committing it, the person was aware of the dangerous nature of the criminal act and desired to engage therein; 2) when committing it, the person was aware of the dangerous nature of the criminal act, anticipated that his act or omission might cause the consequences provided for by Criminal Code of the Republic of Lithuania and desired that they arise. It is obvious that proving such conditions in case of trespass in the context of the use of, for example, UASs, is actually impossible if the accused denies his intent to gather private information.

Privacy in the context of the use of VIRDs in Latvian domestic law and case-law

Even very geographically, historically and culturally close countries, could have formally quite a different regulation on privacy and its protection. This will be disclosed by analysing Latvian national laws on privacy.

Although the term "privacy" itself is new in Latvian law, it cannot be said that the institute of privacy is not known (Torgans, Karklinš, and Bitans, 2017, p. 351). The right to the protection of private life in Latvia is protected by the legal act of supreme power – the Constitution (Lat. *Latvijas Republikas Satversme*, hereinafter - "Latvian Constitution"), more specifically, Article 96: „Everyone has the right to inviolability of his or her private life, home and correspondence"; Article 89: „The State shall recognise and protect fundamental human rights in accordance with this Constitution, laws and international agreements binding upon Latvia" (Latvijas Vestnesis, 1993). In explaining the concept of privacy the Constitutional court of the Republic of Latvia, by quoting a doctrinal source, confirmed that the right to a private life means an individual's right to its private home, his right to live as he likes, in accordance with his nature and wish to develop and improve the personality, tolerating minimum interference of the state or other persons. The Court has also stated that this right includes the right of an individual to be different, retain and develop virtues and abilities, which distinguish him from other persons and individualizes him (Loucaides, 1991, p. 191; Constitutional Court of Latvia, 2004). The

[11] *A. A.*, the decision of the Supreme Court of Lithuania of of 29.11.2018, case No. 2K-348-648/2018, point 7: the court in this case stated that the composition of the crime provided for in Article 167 of the Criminal Code is formal, i.e. the crime is treated as committed completing acts by which information about a person's private life was unlawfully collected (see also *P. K.*, the decision of the Supreme Court of Lithuania of 06.05.2014, case No. 2K-213/2014); *V. B.*, the decision of Kaunas district Court of 19.05.2015, case No. 1S-875-245/2015: the composition of crime provided for in Article 168 is formal; in one of its cases in terms of Article 165 application the Supreme Court of Lithuania stated that: „The moment of entry is also related with the finality of the crime (formal composition of the crime). In order to arise criminal liability it is necessary to also determine the person's fault – direct intent, i. e. the person's awareness of the fact that he/she against the will of the owner or persons authorised unlawfully intrudes on another person's dwelling, apartment or other dwelling or its accessories, including a protected housing area, and wanting to do so" *(A. M.*, the decision of the Supreme Court of Lithuania of 27.01.2015, case No. 2K-37-942/2015).

Constitutional Court of the Republic of Latvia has also described the protection of private life as covering physical and moral integrity, honour and reputation, use of person's name and identity, personal data of a person, and concerning other aspects, connected with private life (Constitutional Court of Latvia, 2009). Furthermore, the Constitutional Court, by reflecting the ECHR case-law, has stressed that the rights guaranteed in Article 96 of the Constitution are not absolute as Article 116 of the Constitution provides that these rights may be subject to restrictions in circumstances provided for by law if it has a legitimate objective and is proportionate (Constitutional Court of Latvia, 2006).

Privacy protection is regulated by a large number of laws and regulations, even though not all of them contain the clearly expressed term "privacy" (Torgans, Karklinš and Bitans, 2017, p. 351). A few of them, that could be related to the use of VIRDs, are mentioned hereinafter. Article 9 of the Law on the Protection of the Children's Rights states that a child has the right to privacy, living quarters, the confidentiality of correspondence, and inviolability and freedom of the person (Latvijas Vēstnesis, 1998a). Freedom of Information Law states that restricted access information is which concerns the private life of natural persons (Latvijas Vēstnesis, 1998b), whereas Article 8 of the same law reaffirms that information regarding the private life of a natural person is protected by law. The most detailed regulation on personal data protection in Latvia is set in the recent Personal Data Processing Law (Latvijas Vēstnesis, 2018), which since 5th July 2018 replaced Personal Data Protection Law (.Latvijas Vēstnesis, 2000). The predecessor, contrary to the Lithuanian situation, did not set any special conditions under the existence of which precisely video surveillance was allowed (only Article 7 obliged to make sure that at least one of the six conditions exists in order to generally process personal data). Whereas in the new Latvian law – Personal Data Processing Law, a separate article is dedicated precisely to the conditions of video surveillance and it says that "The requirements of this Law and the Data Regulation do not apply to the processing of data by natural persons using automated video surveillance devices for personal or household purposes," unless such surveillance is of public space on a large scale or when technical aids are used for the structuring of information (Article 36, part 2). Thus, the provision does not only set the rules on video surveillance but also confirms the specificity of VIRDs as data collection devices.

What is interesting that even though Latvian laws, on the contrary to Lithuanian, do not explicitly distinguish a person's right to an image (including his/her right to expressively disagree of being filmed), but, again, on the contrary to Lithuanian regulation, they clearly state that records obtained in road traffic cannot be disclosed to other persons and institutions (except for separately indicated cases) (Article 36, part 2 of Personal Data Processing Law). The legislator probably had in mind records taken by dashboard cameras. However, as the law does not clearly name the device used in road traffic, this article should be applicable in cases if the UAS was used, for example, to follow a car. Furthermore, the same article also states that it is prohibited to disclose the records obtained in road traffic to other persons and institutions, except when one of the bases of data processing specified in the data regulation is found (see GDPR Article 6 part 1), whereas neither Lithuanian Civil Code nor Lithuanian LPDLP, protect privacy subjects from their images, taken in public – road traffic, being disclosed to others if they do not harm the subjects' reputation, honour, dignity (as indicated in Article 2.22 part 2 of the Civil Code of the Republic of Lithuania). Thus, if a VIRD in traffic recorded a video in which a person could be recognized and this video/photo was made public, under Lithuanian law, no offence is made, as the dignity, honour, and reputation of the person in the video has not been breached. So, it could be said that the person was filmed without even knowing it and without being able to express his disagreement with the process even though he or she did not

want to be recognized as being in a particular place at the particular time or driving a/sitting in a particular car. Whereas the Latvian Personal Data Processing Law ensures such protection.

Furthermore, the Latvian Civil Law, on the contrary to Lithuanian, does not govern privacy questions at all. It only contains provisions on non-pecuniary and pecuniary damage (Government Gazette, 1937). Article 1635 of the Latvian Civil Law states that any violation of rights, that is, any unauthorized act in itself, resulting in harm (including non-pecuniary damage), entitles the victim to seek satisfaction from the aggrieved person to the extent that he or she can be blamed. Privacy-related criminal offences are not among those resulting in presumable non-pecuniary damages, therefore they have to be proved by the claimant (Article 1635). Latvian Civil Law also divides fault into two categories: expressed by intention (i.e. "malicious fault") or negligence (Article 1642), whereas negligence is gross and minor (Article 1644). Therefore in terms of damages and other civil law consequences, gross negligence is tantamount to malicious intent (article 1645). However, in actions arising solely from a breach of law and without prejudice to a pre-existing relationship, the infringer is liable for every negligence, even minor (Article 1649). Therefore it could be concluded that any infringement of privacy-related legal provision in the use of VIRD could result in an award of non-pecuniary damage despite the degree of fault.

After the Latvian Administrative Violations Code ceased to be in force (Latvijas Padomju Sociālistiskās Republikas Augstākās Padomes un Valdības Ziņotājs, 1984), administrative violations and the penalties applicable to them have been specified in the laws and binding regulations of local governments. As the directly applicable legal acts of the European Union and international agreements binding on Latvia, which regulate administrative liability, are a part of the system of administrative liability in Latvia, the field of data protection is governed *inter alia*, by GDPR. This regulation is also directly applicable and provides not only rules of conduct but also sanctions for non-compliance.

Besides, the right to respect for private life which could be breached by the use of visual information recording devices is also protected by the Criminal Law of Latvia, which criminalizes Persecution (Article 132 (1)) (Latvijas Vēstnesis, 1998c), the Transgression of Inviolability of the Dwelling of a Person (Article 143) and illegal activities with personal data (Article 145). An important factor to consider that these crimes, as well as in Lithuanian Criminal Code enshrined the above-mentioned privacy-related crimes could be committed only intentionally (Krastiņš, Liholaja, 2018, p. 70). This factor is important as proving the intent of the suspect is quite complicated in criminal proceedings. It is also important to stress that Latvian case law and scholars have not yet confirmed that entering a private territory with the help of a device (for example UAS) is treated as trespass, therefore it is still held that the person himself/herself has to enter the private territory in order the crime to be committed (Krastiņš, Liholaja, 2016, p. 352).

Latvia, as well as Lithuania, does not have separate regulations on the use of dashboard cameras but on the contrary to Lithuania, has separate national regulation on the operation of UAS (Procedures for Unmanned Aircraft and Other Aircraft Flights [Latvijas Vēstnesis, 2019b]), which, besides reflecting main provisions of Regulation 2019/947, also supplement them. For example, the Procedures state that the operations of unmanned aircraft and aircraft shall be conducted in such a way as not to endanger, besides other values, privacy. Also, the Procedures contain another provision that may indirectly serve for the protection of privacy and prevention of breaches against it is the flight ban between 30 minutes after sunset until 30 minutes before sunrise. This is an important rule helping to avoid secret surveillance from a UAS because it is more difficult to notice and identify the device and its owner in the dark. Finally, commendable is the provision prohibiting to perform flights of UASs closer than 2 m

in the horizontal plane from the street edge of populated areas (towns and villages). The following point sets an exception to the flights over the infrastructure objects or engineering structures and allows them without the consent of the owner or possessor in case if the UAS with the total take-off mass not exceeding 1.5 kg, to fly not less than 50 m above the ground or water surface.

Even though Lithuanian rules for the use of unmanned aircraft ceased to be in force on 01.01.2021 as well as Latvian Procedures for Performing Flights of an Unmanned Aircraft or Movements of Other Such Type of Machine, which are not Classified as Aircraft did on 17.08.2019 (Latvijas Vēstnesis, 2016), it is interesting to compare both states' foresight on the privacy protection from the very beginning of the creation of national rules related to the use of UASs.

On the contrary to Lithuanian rules, Latvian procedures at least mentioned the respect for privacy in the course of the use of the UAS: "Unmanned aircraft flights shall be performed so as not to endanger human life, health, privacy or property, flight safety, and security, not to cause harm to the environment, and also not to endanger the State defence and security interests" (Latvian Procedures for Performing Flights of an Unmanned Aircraft or Movements of Other Such Type of Machine, point 8). Latvian procedures demonstrated the State's willingness to make privacy protection in the use of UAS not only formal but actually working: on the contrary to Lithuanian rules, the formerly mentioned Latvian procedures contained provisions obliging the owner of the UAS to label the device with the given name and surname (for legal persons - company name) of the owner or possessor thereof, address of the declared place of residence (for legal persons - legal address) and phone number. This obligation was far-sighted at the moment of adoption of the procedures as it almost corresponded with the requirements set in the recent Regulation 2019/947 (to make sure that the UAS is identifiable), which came into force much later than the UA Rules (only the condition to indicate the registration number was missing in the former).

Also, the UA rules obliged the controller of unmanned aircraft to be identifiable (Latvian Procedures for Performing Flights of an Unmanned Aircraft or Movements of Other Such Type of Machine, point 28). These requirements ensured easier determination and identification of the person managing the UAS in cases when there was a question of any kind of liability and in such a way at least partly served not only for safety insurance but for privacy protection as well (when the responsible person concerning privacy breaches would have had to be found or illegal observation of private areas would have had to be interrupted). These requirements were useful and practical steps towards realistic, not only formal, implementation of privacy protection. However, modelling a situation that a person breaches the requirements for the device and self-identification assurance, it would have still been very hard to identify the offender (in case of privacy breaches when using UAS). When Lithuania has not yet adopted any specific national measures on privacy protection in the use of UAS and Latvian Procedures for Unmanned Aircraft and Other Aircraft Flights are valid until 01.07.2021, only the future will show how successfully both countries: Latvia and Lithuania will enforce the requirements of Regulation 2019/947 and adapt to their national understanding of privacy. However, Latvia is one step ahead here.

Privacy protection in the use of VIRDs by Police

Procedural measures involving the recording of visual information in criminal intelligence, preliminary investigation touch mainly precise people who might have been involved in criminal actions. Such procedures related to limiting protection of privacy allow for

a very broad margin of appreciation (*Uzun v. Germany, 2010; Murray v. the United Kingdom, 1994)*. Whereas activities related to ensurance of public order, on the contrary, should be much better balanced in terms of privacy protection and aims sought. Furthermore, the scale of people affected by the usage of VIRDs (precisely, dashboard cameras, UASs) is incomparably larger because it affects or may affect any person in a public place.

UASs could be used by the police – for search, ensuring public order (for example, at mass events), whereas dashboard cameras are mounted in police cars and police patrols carry out continuous surveillance of public places and video recording in files. Video recording by the police or other resembling authority is necessary because it can increase public safety and may assist in the investigation of any type of offence. Even "visible recording can also deter certain people from engaging in criminal acts" but if not carried out sensitively, "it can lead to intimidation of participants" (Murdoch, Roche, 2013, p. 107).

The use of UAS by the police is not that problematic in terms of privacy as such use is not covert (presuming that the persons observed see the UAS being used) and also not of permanent and systematic nature. It should be mentioned that there is no data on the use of UASs in police activities, frequency of such use, therefore deeper analysis could not be carried out. But talking about dashboard cameras mounted in police cars, it could be stressed that the surveillance by this type of VIRDs is of permanent and systematic nature, as probably all public police cars are equipped with this type of VIRD. This means that such surveillance could fall into the scope of Article 8 of the Convention, therefore must comply with a range of the earlier mentioned conditions which are: the interference must be in pursuance of a legitimate aim; it must be in accordance with the law, and it must be necessary in a democratic society. The non-existence of any of these conditions makes the use of the VIRD unjustified, in other words, such use would be treated as a violation of Article 8 of the Convention. It would not be difficult to prove that the surveillance by a dashboard camera is pursuant to a legitimate aim (insurance of public safety, crime prevention) and is necessary in a democratic society, therefore it is necessary to analyse whether it is in accordance with the law.

Before analysing the publicly accessible internal rules concerning the approval of image data, it is necessary to stress that police activities related to processing personal data are also governed by national laws derived from EU regulations – GDPR (if Member States have entrusted competent authorities with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, fell within the scope of GDPR (Regulation (EU) 2016/679, 2016) and Directive (EU) 2016/680 (2016), that are the earlier-mentioned LPDLP and The Law on personal data, processed for the prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties or national security or defence, legal protection. The latter, among other purposes, is also applied to the processing of personal data by the competent authorities of the Republic of Lithuania where such processing is for the prevention, investigation, detection, or prosecution of criminal offences or the execution of penalties, as well as protection against and prevention of threats to public security and enshrines principles of personal data processing, such as a none-excessive collection of personal data for a specified, explicit and legitimate purpose, keeping the data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed, and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. In other words, the law reflects the main conditions

(permissible interferences) and principles of application of a margin of appreciation in the context of privacy protection (such as lawfulness, proportionality, necessity, etc.).

When analysing whether the above-mentioned privacy-related principles are met in terms of video surveillance by police, it could be said that the compliance of the principle of lawfulness ("in accordance with the law") is implemented by the Police Law of the Republic of Lithuania (Valstybės žinios, 2000), Article 22 part 1 clause 12, which enshrines police officer's right to take pictures or video recordings with the consent of the person or/and in cases established by law. Using dashboard cameras in police cars or UASs is not reconcilable with the requirement of reception of a person's consent (because it is practically impossible). However, such use could be treated as being carried out on the grounds established by law. Specifications for Special Remedies and Procedures for the Use of Special Remedies, approved by the Resolution of the Government of the Republic of Lithuania (2016) treats dashboard cameras (even though not specifically mention them) and UASs as special measures, point 2.14 states that "Remote sensing Measures are unmanned aircraft, vehicles <...> or other technical means autonomous or remotely operated, for the purpose of capturing offenses, monitoring a group of persons". Special measures are one of the categories of "physical abuse" allowed for the police (Article 2 part 2 of the Police Law). The Procedures for the Use of Special Measures indicate that the conditions and grounds for the use of the special measures shall be laid down, among others, in the Police Law of the Republic of Lithuania, whereas The Police Law states that the grounds for application of physical abuse (including special measures), among others, are the protection of others against imminent danger to life or health, prevention of administrative misconduct or criminal activity. Thus, if a dashboard camera is treated as a special measure (taking into consideration that the UASs are, looks like dashboard cameras are treated as such as well, if not – it could be treated that the grounds for their use are not set in any law), it could be said that the criteria of lawfulness are satisfied, or at least the application of such measure is foreseeable because both the above-mentioned laws precisely indicate the grounds of the use of special measures. As it was mentioned, the requirement of "in accordance with the law" must satisfy foreseeability sub-criteria which means that the law should be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which public authorities were empowered to resort to the interference with the right to respect for private life, it is confirmed by European Court of Human Rights practice (ECHR Research Division (2013); *Shimovolos v. Russia* (2011)).

Furthermore, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of abuse of power, compatibility with the rule of law requires domestic law to provide adequate protection against arbitrary interference with Article 8 rights and such protection, among others, also include the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (as in *Vukota-Bojić v. Switzerland* (2016); *Uzun v. Germany* (2010). Even though the latter interpretation is formulated by the ECHR in the context of secret surveillance, and video surveillance by Public Police is not treated as such but considering the specificity of UASs (that their operation is not easily noticeable) and also considering the specificity of VIRD's operator (that it is a police – a public authority), the criteria of supervision of the use of VIRDs and requirement of remedies are applied.

Police Commissioner-General of the Republic of Lithuania has approved the rules "On image data, captured by the image monitoring means handling in police offices" (2015). The rules are intended to assure that the image data-related activities are carried out in accordance with the EU law and national laws derived from it (most importantly, data protection). The rules set the list of persons that are allowed to process visual data (point 13), sets the maximum term

of visual data captured by VIRDs storage which is 60 days (point 38), provides automatic deletion of visual data after its term of storage or familiarisation expires (points 40, 46), enshrines the requirement if possible to inform the persons whose data are collected that video data is being recorded (point 32). In other words, this by-law enshrines remedies for proper management of visual data in police.

Thus, it could be said that the requirement of "in accordance with the law", applicable for the permissible interferences to the right to privacy, set by the ECHR, is met in case of VIRDs surveillance by the police of Lithuania as it sets the grounds for use of such a measure (but only if presumed that dashboard cameras were treated as special measures) and also sets the remedies for lawful processing of personal data.

The use of VIRDs in the activities of police would also pass a test of justification of margin of appreciation set by the ECJ as the measure (visual data collection by VIRDs) limits EU fundamental rights (such as the right to privacy and protection of personal data), the limitation is allowed as these two rights are not absolute, the limitation is provided by law (criteria of foreseeability is satisfied), respect of these rights are guaranteed (remedies are set, such as prior warning about personal data being captured, a limited term of data storage, limited access to the data, automatic deletion, the limitation serves a legitimate objective (as stated in the Police Law or in the rules) (point 10), it is suitable to consistently and systematically meet the objective pursued (there is a set of just-mentioned complementary laws), there are no any measures available that would interfere less (considering the advances in modern technologies and their benefits, there are no other means capable of achieving at least similar results).

Moreover, it is important to stress that the rules "On image data, captured by the image monitoring means handling in police offices" include provision obliging Public Police buildings and cars equipped with dashboard cameras, to be marked with the signs warning about ongoing video surveillance (point 7). The cars must be marked inside the cabin as well as outside on the front, rear, and sides of the car body. Such a requirement is important to ensure the persons concerned the possibility to exercise their rights provided in GDPR and are informed about the surveillance and derivative national laws. However, it has to be not only formal but implemented in practice.

Police Law of the Republic of Latvia (1991) also includes provisions related to visual data capture and sets the main relevant rules in the law itself. The law states that restrictions on the rights and freedoms of individuals are permissible only based on and in accordance with the law, consequently (Article 5, Part 4), whenever the police apply such restriction, the police officer has to give them an explanation justifying each specific restriction. The law also enshrined police officer's right to observe public places and persons in them, by using technical means for the timely prevention and detection of a possible public order threat, crime, finding persons or vehicles searched, as well as observing the buildings, premises of police institutions by technical means and the territory, police guarded objects, to ensure the security of the buildings, premises, and territory of the police authorities, the security of detained persons and guarded objects (Article 12, Part 14). The law also obliges the Cabinet to determine procedures of surveillance carried out by technical means, as well as the rules on processing the data obtained as a result of such surveillance (Article 12). Furthermore, the Law On Processing of Personal Data in the Criminal Proceedings and Administrative Offence Proceedings (2019a) states that the purpose of this Law is to protect the fundamental rights of natural persons, in particular the inviolability of private life, during the processing of personal data by competent authorities in order to (among others) prevent, investigate and detect criminal offences and administrative offences perform other activities related to administrative offence proceedings or criminal proceedings.

The implementing by-law – "Procedures for police surveillance by technical means and the processing of data resulting from such surveillance" (2017) sets the maximum term of retention of observation data, which is three months (except the cases when the data identify a threat to public order, a criminal offence, the person or vehicle being searched, etc. – can be kept for a maximum of three years). Furthermore, the procedures also oblige that the surveillance shall be warned using an informative sign (Article 8) which in case of dashboard cameras mounted in police cars has to be placed "in a conspicuous place" (Article 9). From this wording, it is not clear whether the sign has to be placed on the body of a car or inside it and to whom this sign must be visible: to any person outside the car or the person sitting in the police car. It is also stressed that the surveillance shall not take place in places where individuals expect a particularly high level of privacy protection. However, it is not clear, what conditions allow to determine that the place is the one with high expectation of privacy. Of course, the highest level of privacy for any individual is expected at home, however, the procedures are designed to regulate surveillance in public places, therefore home cannot be the object described by this provision. Even though formally Latvian laws also could be treated as meeting the requirements of the test of justification of margin of appreciation but the above-mentioned provisions concerning marking of police cars with a sign of surveillance being carried on and places of high expectation of privacy protection should be more detailed in order to be effective in privacy protection.

Conclusions

Specific area of the protection of privacy is law enforcement national authorities whose privacy protection specifics cannot be analysed because of the inaccessibility of internal legislation governing the processing of personal data in criminal intelligence. However, as the brief analysis of regulation on VIRD use in the Police disclosed, both: Lithuanian and Latvian regulation have small inaccuracies that need to be fixed. Despite the usefulness of VIRDs in the police, the most important rules should not be forgotten: a publicly-available policy on how video recordings are made and retained should be in place; footage should only be used for criminal investigations, and should not be retained for longer than necessary (Murdoch, Roche, 2013, p. 107). If the footage is retained for longer than required and is stored in such a way that individuals can be identified from it, it may result in a violation of the right to respect for private life (as guaranteed by Article 8 of the Convention). Regulation on the use of VIRDs in police is not clear enough in both countries. In Lithuania there is a lack of clearance of the term "special measure" the interpretation of which may lead to the nonconformity with the "lawfulness" requirement set by the ECHR, whereas Latvian regulation on the topic lacks clearance in the provisions of "place of particularly high expectation of privacy" in which the surveillance is not allowed and "conspicuous place" in which the sign informing about ongoing visual information recording has to be placed.

References

1. 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*. Available at: https://time.com/5735411/china-surveillance-privacy-issues/ (Accessed: 25 December 2019)
2. Directive (EU) 2016/680 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 by

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

3. Douglas v. Hello! (2005) EWCA Civ 595; [2006] QB 125; [2005] 3 WLR 881; [2005] EMLR 609; The Times 24 May 2005; The Times 26 May 2005. Available at: https://swarb.co.uk/douglas-and-others-v-hello-ltd-and-others-no-3-ca-18-may-2005/ (Accessed: 05 June, 2021)
4. ECHR Research Division (2013). *National security and European Case-Law*. Available at: https://rm.coe.int/168067d214 (Accessed: 23 February, 2019);
5. European Court of Human Rights. (2010). 50 Years of Activity. Available at: https://www.echr.coe.int/Documents/Facts_Figures_1959_2009_ENG.pdf (Accessed: 01 May 2017)
6. 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.
7. Krastiņš, U., Liholaja, V. (2018). *Krimināllikuma komentāri*, *Pirmā daļa (I-VIII2). Otrais papildinātais izdevums.* Rīga: Tiesu namu aģentūra, p. 70.
8. Krastiņš, U., Liholaja, V. (2016). *Krimināllikuma komentāri. Otrā daļa (IX-XVII nodaļa)*. Rīga: Tiesu namu aģentūra, pp. 341, 352.
9. Loucaides, L. G. (1991). Personality and privacy under the European Convention on Human Rights. *The British Yearbook of International Law*. Oxford: Oxford University Press, p. 191;
10. Murdoch, J., Roche, R. (2013). The European Convention on Human Rights and policing. Available at: https://www.echr.coe.int/Documents/Handbook_European_Convention_Police_ENG.pdf, p. 107 (Accessed: 01 January, 2020).
11. 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.
12. Pranevičienė, B. (2011). Limiting of the Right to Privacy in the Context of Protection of National Security. *Jurisprudence*, 18(4), p. 1613.
13. Puraite, A., Bereikiene D., Silinske, N. (2017). Regulation of Unmanned Aerial Systems and Related Privacy Issues in Lithuania, *Baltic Journal of Law and Politics*, Vol. 10, p. 118.
14. 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, p. recital, point 19.
15. Solove, D. (2009). *Understanding Privacy*. Cambridge, Massachusetts London, England: Harvard University Press, p. 2.

16. 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. 351.

Latvia's legal regulation and case-law

17. Constitutional Court of Latvia (2009) The judgment of the Constitutional Court of Latvia of 23.04.2009, Case No. 2008-42- 01.

18. Constitutional Court of Latvia (2006) The judgment of 26 January 2006 by the Constitutional Court of Latvia, case No. 2004 -17-01.

19. Government Gazette (1937) The Civil Law (Civilikums). Adopted on 28.01.1937. Published: Government Gazette, 41, 20.02.1937. Last amendments 29.10.2015, Article 1635.

20. Latvijas Padomju Sociālistiskās Republikas Augstākās Padomes un Valdības Ziņotājs (1984) Latvian Administrative Violations Code (Latvijas Administratīvo pārkāpumu kodekss). Adopted on: 07.12.1984. Published: Latvijas Padomju Sociālistiskās Republikas Augstākās Padomes un Valdības Ziņotājs, 51, 20.12.1984. Ceased to be in force on 01.07.2020.

21. Latvijas Republikas Satversme (1993) Latvijas Vēstnesis, 43, 01.07.1993.; Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 6, 31.03.1994.; Valdības Vēstnesis, 141, 30.06.1922.; Diena, 81, 29.04.1993.

22. Latvijas Vēstnesis (1998a) Law on the Protection of the Children's Rights (Bērnu tiesību aizsardzības likums). Adopted on 19.06.1998. Published: Latvijas Vēstnesis, 199/200, 08.07.1998.

23. Latvijas Vēstnesis (1998b) Freedom of Information Law (Informācijas atklātības likums). Adopted on 29.10.1998. Published: Latvijas Vēstnesis, 334/335, 06.11.1998; Reporter of the Saeima and the Cabinet of Ministers of the Republic of Latvia, 24, 24.12.1998. Last amendments 03.09.2015, Article 5, part 2, clause 4.

24. Latvijas Vēstnesis (1998c) 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 132 (1).

25. Latvijas Vēstnesis (2000) Personal Data Protection Law (Fizisko personu datu aizsardzības likums). Adopted on 23.03.2000. Published: Latvijas Vēstnesis, 123/124, 06.04.2000; Reporter of the Saeima and the Cabinet of Ministers of the Republic of Latvia, 9, 04.05.2000. Ceased to be in force on 05.07.2018.

26. Latvijas Vēstnesis (2016) The Procedures for Performing Flights of an Unmanned Aircraft or Movements of Other Such Type of Machine, which are not Classified as Aircraft (Kārtība, kādā veicami bezpilota gaisa kuģu un tādu cita veida lidaparātu lidojumi, kuri nav kvalificējami kā gaisa kuģi). Adopted on 22.11.2016. Published: Latvijas Vēstnesis, 231, 28.11.2016. Ceased to be in force on 17.08.2019.

27. Latvijas Vēstnesis (2017) Procedures for the performance of surveillance by the police by technical means, as well as the processing of data obtained as a result of such surveillance (Kārtība, kādā policija veic novērošanu, izmantojot tehniskos līdzekļus, kā

arī šādas novērošanas rezultātā iegūto datu apstrādi). Adopted on 21.03.2017. Latvijas Vēstnesis, 61, 23.03.2017.

28. Latvijas Vēstnesis (2018) Personal Data Processing Law (Fizisko personu datu apstrādes likums). Adopted on 21.06.2018. Published: Latvijas Vēstnesis, 132, 04.07.2018. Last amendments 23.05.2019.

29. Latvijas Vēstnesis (2019a) On Processing of Personal Data in the Criminal Proceedings and Administrative Offence Proceedings (Par fizisko personu datu apstrādi krimināl procesā un administratīvā pārkāpuma procesā). Adopted on 08.07.2019. Published: Latvijas Vēstnesis, 147, 22.07.2019.

30. Latvijas Vēstnesis (2019b) Procedures for Unmanned Aircraft and Other Aircraft Flights (Kārtība, kādā veicami bezpilota gaisa kuģu un cita veida lidaparātu lidojumi). Adopted on 13.08.2019. Published: Latvijas Vēstnesis, 166, 16.08.2019. Valid until 01.07.2021.

31. Reporter of the Supreme Council and Government of the Republic of Latvia (1991) Law on Police (Par policiju). Adopted on 04.06.1991. Published: Reporter of the Supreme Council and Government of the Republic of Latvia, 31/32, 15.08.1991; Day, 126, 05.07.1991. Last amendments 14.03.2019.

Lithuania's legal regulation and case-law

32. Constitutional Court of the Republic of Lithuania (2002) The ruling of the Constitutional Court of the Republic of Lithuania of September 19, 2002 *On the Law on Telecommunications, the Law on Operational Activities, and the Code of Criminal Procedure*, case No. 34/2000-28/01.

33. Kaunas District Court (2015) Case No. 1S-875-245/2015, 19.05.2015.

34. Klaipeda District Court (2011), Case No. 1A-358-360/2011, 16.06.2011.

35. Official Gazette (1992) Constitution of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos Konstitucija), Official Gazette (1992), no. 220, 33-1014.

36. Official Gazette (2000) Law on Personal Data Legal Protection of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas), Official Gazette, No. 63-1479; 2000, No. 64-1924; 2003, No. 15-597; 2008, No. 22-804; TAR, 2018-07-11, No. 2018-11733.

37. Official Gazette (2000), Civil Code of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos civilinis kodeksas), 18.07.2000 Lithuania, Official Gazette (2000), No. 74-2262.

38. Rules on image data, captured by the image monitoring means handling in police offices (Lithuania), (Vaizdo stebėjimo būdu užfiksuotų duomenų tvarkymo policijos įstaigose taisyklės). Adopted on 28.10.2015. Order of Police Commissioner General of the Republic of Lithuania, No. 5-V-963, amended by 18.10.2019 order No. 5-V-783. 02.05.2020 Available at: http://lpm.policija.lrv.lt/uploads/lpm.policija/documents/files/result(10).pdf (accessed 02 May, 2020).

39. Supreme Court of Lithuania (2013) The ruling of the Supreme Court of Lithuania of 23.04.2013, Case No. 2K-198/2013.

40. Supreme Court of Lithuania (2014) The ruling of the Supreme Court of Lithuania of 06.05.2014, Case No. 2K-213/2014.

41. Supreme Court of Lithuania (2015) The ruling of the Supreme Court of Lithuania of 27.01.2015, Case No. 2K-37-942/2015.

42. Supreme Court of Lithuania (2018) The ruling of the Supreme Court of Lithuania of 29.11.2018, Case No. 2K-348-648/2018.

43. TAR, (2014) The rules for the use of unmanned aircrafts (Lithuania), (Bepiločių orlaivių naudojimo taisyklės), 23.01.2014 Vilnius, TAR, 2014, No. 2014-00438. Ceased to be in force on 01.01.2021.

44. TAR (2015) Code of Administrative offences of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos administracinių nusižengimų kodeksas), 25.06.2015 Lithuania, TAR, 2015-07-10, No. 2015-11216.

45. TAR (2016) Specifications for Special Measures and Procedures for the Use of Special Measures (Specialiųjų priemonių specifikacijos ir Specialiųjų priemonių panaudojimo tvarkos aprašas) (Lithuania), 23.11.2016 Vilnius, TAR, 2016-11-28, No. 27588.

46. TAR (2020a) Order of Director of Lithuania transport safety administration of 24.09.2020 No. 2BE-309 "On approval of the Description of the Unmanned Aircraft Market Surveillance" (Lietuvos transporto saugos administracijos direktoriaus 2020 m. rugsėjo 24 d. įsakymas No. 2BE-309 „Dėl Bepiločių orlaivių rinkos priežiūros tvarkos aprašo patvirtinimo"), Lithuania, TAR (2020), No. 2020-19818.

47. TAR (2020b) Order of Director of Transport Competence Agency of 30.12.2020 No. 2-308 "On approval of the Description of the Procedure for the issuance of qualification documents to a remote pilot of unmanned aerial system" (Viešosios įstaigos Transporto kompetencijų agentūros direktorius 2020 m. gruodžio 30 d. įsakymas No. 2-308 „Dėl Bepiločio orlaivio sistemos nuotoliniam pilotui išduodamų dokumentų, patvirtinančių jo kvalifikaciją, tvarkos aprašo patvirtinimo", TAR (2020), No. 2020-29144;

48. TAR (2020c) Order of Director of Transport Competence Agency of 30.12.2020 No. 2-306 "On the approval of the Description of the Procedure for the Issuance of the Light UAS Operator Certificate" (Viešosios įstaigos Transporto kompetencijų agentūros direktorius 2020 m. gruodžio 30 d. įsakymas No. 2-306 „Dėl Lengvosios bepiločių orlaivių sistemos naudotojo pažymėjimo išdavimo tvarkos aprašo patvirtinimo"), TAR (2020), No. 2020-29139.

49. Valstybės žinios (2000) Police Law of the Republic of Lithuania (Lithuania), (Lietuvos Respublikos Policijos įstatymas), 17.10.2000 Lithuania, Žin., 2000, No. 90-2777; TAR, 2015-07-03, No. 2015-10818.

Case-law of European Court of Human Rights

50. Eerikäinen and Others v. Finland (2009), no. 3514/02, 10 February 2009. Available at: http://hudoc.echr.coe.int/eng?i=001-91242 (Accessed: 05 June, 2021).

51. Murray v. the United Kingdom (1994), no. 300-A. Available at: http://hudoc.echr.coe.int/eng?i=001-57980 (Accessed: 05 June, 2021).

52. Shimovolos v. Russia (2011), no. 30194/09. Available at: http://hudoc.echr.coe.int/eng?i=001-105217 (Accessed: 05 June, 2021).

53. Uzun v. German (2010), no. 35623/05. Available at: http://hudoc.echr.coe.int/eng?i=001-100293 (Accessed: 05 June, 2021).

54. Von Hannover v. Germany (2012), nos. 40660/08 and 60641/08. Available at: http://hudoc.echr.coe.int/eng?i=001-109029 (Accessed: 05 June, 2021).

55. Vukota-Bojić v. Switzerland (2016), no. 61838/10. Available at: http://hudoc.echr.coe.int/eng?i=001-167490 (Accessed: 05 June, 2021).