ISSN 2029-1701
ISSN 2335-2035 (Online)

Mokslinis žurnalas
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2020 (24)
Research Journal

PRIVACY PROTECTION IN THE NEW EU REGULATIONS ON THE USE OF UNMANNED AERIAL SYSTEMS

Aurelija Pūraitė

Mykolas Romeris university Academy of Public Security Department of Law
V. Putvinskio 70, LT-44211 Kaunas, Lithuania
Telephone (+370 37) 303655
E.mail: aurelija_puraite@gmail.com

Neringa Šilinskė

Turiba University Faculty of Law
68 Graudu Street, Riga, LV-1058 Latvia
Telephone +370 600 64460
E. mail:n.silinske@gmail.com

DOI: 10.13165/PSPO-20-24-11

Annotation. The new European Union Regulations on the use of unmanned aerial systems (UASs) is another but not the last step in regulating the use of the technology. One of their purposes is to mitigate risks on privacy and protection of personal data, arising from the operation of UASs. While the 'U-space' system, among others, including remote identification is at the development stage only, privacy-related aspects in the Regulations (EU) 2019/945 and 2019/947 may already be analysed. The authors hold that to achieve effective protection of privacy in the field of the use of UASs, it is essential to ensure effective identification of UAS operator, therefore the exceptions of the requirement to equip the UASs with remote identification add-ons could be a loophole for abuse.

Keywords: unmanned aerial system, privacy, EU.

INTRODUCTION

The abundance of relatively new regulation on data protection (which undoubtedly is closely connected with privacy[1]) (namely General Data Protection Regulation, hereinafter – GDPR) (European Parliament, Council 2016) and the use of unmanned aerial systems (hereinafter – UASs) at the European Union (hereinafter – EU) level proves the existence of a threat to privacy that is being caused by the modern technologies. For example, recital of the General Data Protection Regulation (hereinafter - GDPR) which came into force a few years ago, states: "*Rapid technological developments and globalisation have brought new challenges for the protection of personal data".* Recital of the Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft

[1] Despite the distinction between privacy and data protection laid down in the Charter, the jurisprudence has justifiably considered privacy to be at the core of data protection (Kokott, Sobotta 2013).

(hereinafter – Regulation 2019/947) also stresses the risks to privacy and protection of personal data that are caused by the operation of UASs equipped with sensors able to capture personal data (European Commission 2019b). The specificity of the use of UASs and the threat to privacy caused by it could be confirmed by the fact that recital of Regulation (EU) 2018/1139 distinguishes the use of UASs in a separate paragraph and states that „the rules regarding UAS should contribute to achieving compliance with relevant rights guaranteed under Union law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to protection of personal data, set out in Article 8 of that Charter and Article 16 TFEU, and regulated by Regulation (EU) 2016/679 of the European Parliament and the Council" (European Parliament, Council 2018). The EU legislation is a constituent part of the legal systems of Member States and has supremacy over the national laws (Mikelsone 2013), therefore, it could be said that the most detailed regulation on the protection of privacy when using unmanned aerial systems (hereinafter – UASs), also data protection is set at the European Union level.

Even though the Regulation 2019/947 is in effect and shall apply from 1 July 2020, Lithuania has not yet harmonised its national "Rules for the use of unmanned aircrafts" (2014) with the new EU regulation, but it will have to be done sooner or later. The authors aim to determine how effectively privacy is protected in the context of the use of UASs at the EU level, precisely in the recent Regulation 2019/947. Such systematic analysis is timely as it could serve for the adoption of national laws related to the use of UASs. To achieve the aim not only Regulation 2019/947 but also Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and third-country operators of unmanned aircraft systems (European Commission 2019a) (hereinafter – Regulation 2019/945) is analysed, as the latter lays down the requirements for remote identification of UASs, which is very important in helping to determine the operator of the UAS and, accordingly, together with other factors, serves for more effective privacy protection in the use of UASs.

THE MAIN THEORETICAL ASPECTS OF THE EU REGULATIONS ON THE USE OF UASs

EU legislation connected with UASs is quite comprehensive. Before moving to specific regulation on the use of UASs, it is also necessary to mention Regulation (EU) 2018/1139 (European Parliament, Council 2018). Even though this regulation is not dedicated specifically

for the protection of the right to private life, but this legislation, among other rules, is also meant to govern the use of UASs, emphasizes the need for the protection of privacy during such use. The word „privacy" in this legislation is used twelve out of thirteen times particularly in the context of the use of UASs. Thus, the Regulation (EU) 2018/1139 serves for protection of privacy in such use by setting the tasks that should be achieved, which are: to set requirements concerning the registration of UASs and their operators, to establish national registration systems in which basic data of UASs and their operators should be stored; also, by setting the limitation to the application of the Regulation in setting national rules on operations of the UAS for protection of public security, privacy and data protection; by giving precise technological requirements for purposes of privacy, personal data protection, such as easy identification of the aircraft and the nature and purpose of the operation and compliance with limitations, prohibitions or conditions on geographical zones, certain distances from the operator or certain altitudes. Thus, following these aims, Regulations 2019/945 and 2019/947 have been adopted.

Privacy-related "fuses" in the Regulation 2019/945

The recent Regulation 2019/945 which shall apply from 1 July 2020 has divided UASs into classes in terms of their technical characteristics. As in this research privacy question concerns, the table below illustrates the application of the requirement for relevant classes of UASs to be equipped with remote identification add-ons. Such requirement is related with identification of UASs, as without this, considering the specificity of UASs (that there is quite problematic to identify the operator of UAS, to determine the purpose of such operation (Pūraitė, Bereikienė, Šilinskė 2017) liability for the privacy breaches would be impossible. Regulation 2019/945 specifies the requirements for pilots and operators of UASs, also indicates which class UASs have to be equipped with remote identification add-ons. These add-ons allow the upload of the UAS operator registration number, ensures, in real-time during the whole duration of the flight, the direct periodic broadcast from the UAS using an open and documented transmission protocol, of the UAS operator registration number, the geographical position of the UAS and its height above the surface or take-off point, the geographical position of the remote pilot or, if not available, the take-off point (European Commission 2019a).

Depending on the class of the UAS, different technical requirements apply. As Table 1 indicates, it is required that only the UASs of class C1, C2, C3 were equipped with remote identification add-ons.

Table 1. Classes of UASs and the requirement of a direct remote identification equipment

	C0	C1	C2	C3	C4
Direct remote identification add-on	-	+	+	+	-

Source: authors Pūraitė, A., Šilinskė, N.

Whereas there is no such requirement for UASs of class C0 and C4. As the UASs of these two classes are technically simpler than the UASs of class C1, C2, C3, they are more accessible to the majority of people. However, it does not mean that they could be less dangerous in terms of possible privacy breaches as they all are capable of carrying a sensor able to capture personal data.

Privacy protection-related aspects of the operation of UASs in the Regulation 2019/947

Another step in achieving the latter-mentioned tasks enshrined in the Regulation (EU) 2018/1139 is the recent adoption of the Regulation 2019/947 which lays down detailed provisions for the operation of unmanned aircraft systems as well as for personnel, including remote pilots and organisations involved in those operations (European Commission 2019b). This regulation is an important step towards realistic insurance of the protection of privacy in the field of the use of UASs. The Regulation (EU) 2019/947 includes requirements for the implementation of three foundations of the U-space system, namely registration, geo-awareness, and remote identification, which, after fully completed, will solve one of the most important privacy-relating issues – possibility to identify the UAS (and accordingly its pilot/operator), without which, in the authors' opinion, the liability for the breaches of privacy in this field would be impossible.[2] However, rules and procedures for the marking and identification of unmanned aircraft and the registration of operators of unmanned aircraft or certified unmanned aircraft are only to be established therefore their effectiveness conclusively cannot be evaluated at the current stage. Furthermore, it is important to stress that Regulation

[2] Recital point 13 of the Regulation 2019/947 (European Commission 2019b) obliges to establish rules and procedures for the marking and identification of unmanned aircraft and for the registration of operators of unmanned aircraft or certified unmanned aircraft; point 14 of the recital: „operators of unmanned aircraft should be registered where <...> the operation of which presents risks to privacy, protection to personal data...", point 16 of the recital states that if an operator oprates UAS equipped with a sensor able to capture personal data, he/she should be registered considering the risks to privacy and personal data.

2019/947 is without prejudice to the possibility for 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 under the Union law (European Commission 2019b). This is the ground for national authorities to decide on additional rules concerning the use of UASs to assure effective protection of privacy to the extent which is necessary for particular jurisdiction depending on understanding of privacy in that specific state.

Important thing is that concerning privacy protection, the minimum mass of 300 g is no longer relevant (whereas in the national rules such weight is the threshold below which these rules, except for the requirements of maximum flight height, are not applied (The rules for the use of unmanned aircraft 2014). It means that if the UAS is equipped with a sensor able to capture personal data, considering the risks to privacy and protection of personal data, operators of unmanned aircraft should be registered, despite the weight of the UAS. However, this rule is not applied for UASs considered to be toys (European Commission 2019b) within the meaning of Directive 2009/48/EC of the European Parliament and the Council on the safety of toys (European Parliament, Council 2009).

Table 2. The conditions of operation of different class UASs in different „Open“ category flight sub-categories directly or indirectly related to privacy protection

	A1	**A2**	**A3**
Classes of UAS allowed to fly in a particular sub-category	C0, C1 and separately indicated UASs	C2	C2, C3, C4 and separately indicated UASs
Completion of an on-line training course including privacy and data protection questions for pilots required	C1 only	+	+
Requirements for a certificate of remote pilot competency	-	+	-
Overflight of uninvolved persons allowed	C0 and separately indicated UASs	+	+
Operation distance from residential, industrial, commercial, recreational areas is set	-	-	150 meters

Source: *authors Pūraitė, A., Šilinskė, N.*

The Regulation 2019/947 defines three categories of flights and different requirements applied to them: “open”, “specific” and “certified”. The first, “open” category is divided into three sub-categories: A1, A2 and A3, based on operational limitations, requirements for the remote pilot and technical requirements for the UASs

Table 2 demonstrates that the least requirements are set for the flights of A1 category carried out by UASs of the class C0 and A3 category flights operated by UASs of the class C4 (for UASs' class requirements see Table 1). Combining the data presented in Table 1 and Table 2 it could be said that these two types of UASs are the most threatening to privacy because neither class C0 nor class C4 requires the UASs to be equipped with the direct remote identification including direct periodic broadcast functions.[3] Furthermore, the operators/pilots of the flights of A1 category operating C0 class UASs are not required to complete an on-line training course including privacy and data protection questions, overflight of uninvolved persons is allowed (which means that the UAS of such type could be used to record details of persons' private life), operation distance from residential, industrial, commercial, recreational areas is not set (it means that such UAS could be operated in these areas).

Even though A3 category flights require higher competences of the operator (completion of an on-line training course including privacy and data protection questions is required) class C4 UAS, the flights of which are treated as falling under the category of A3 flights, is also not required to have the feature of direct remote identification. Regulation 2019/947 states that the low-risk operations should be allowed to be conducted in the 'open' category because UASs of class C4 is simpler than other classes of UASs, they have achieved the good level of safety, such aircraft are often used by model aircraft operators, therefore, should not be subject „to disproportionate technical requirements" (European Commission 2019b). Provided that UAS of class C4 is equipped with a photo/video camera, there is a trace of safeguard of privacy applicable in the situation like this in the point 14 and 16 of the recital of Regulation 2019/947 which obliges operators of UASs to be registered if they operate an unmanned aircraft, operation of which presents risks to privacy, protection of personal data, security or the environment, in other words, if the UAS in operation is equipped with a sensor able to capture personal data (European Commission 2019b).[4] However, it is questionable whether the latter provision could serve for the protection of privacy. Even though the rules and procedures for

[3] This function ensures, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, of the following data, in a way that they can be received directly by existing mobile devices within the broadcasting range: the UAS operator registration number, the unique physical serial number of the UA, the geographical position of the UA and its height above the surface or take-off point, the route course measured clockwise from true north and ground speed of the UA, the geographical position of the remote pilot (European Commission 2019a).

[4] However, this should not be the case when the unmanned aircraft is considered to be a toy within the meaning of Directive 2009/48/EC (European Parliament, Council 2009).

the registration of operators of unmanned aircraft are only to be established, and evaluation of their effectiveness is currently impossible but already now the question how the registration of operators, for example, of UASs of class C4, could serve for privacy protection if, for example, UASs of class C4 do not have remote identification function, arises.

The table 2 shows that the least requirements are set for the flights operated by UASs of class C0 and C4 respectively in A1 and A3 subcategories of the „Open“ category of flights not only because UASs of these classes are not required to be equipped with remote identification add-ons, but also because the operations in earlier-mentioned sub-categories almost do not have restrictions. It is also important to note that „open“ category flights do not require any prior authorization or operational declaration (European Commission 2019b).

As further will be seen, all the abovementioned factors play a role in evaluating the effectiveness of the legislation in terms of privacy protection but also in the determination of possible ways to breach privacy and, accordingly, liability questions.

OTHER PROBLEMATIC ASPECTS OF PRIVACY PROTECTION IN THE REGULATIONS 2019/945 AND 2019/947 AND SUGGESTIONS FOR THEIR CORRECTION

As Regulation 2019/947 has come in force, the foundation for the effectiveness of privacy protection in the field of the use of UASs has been laid down. The most important thing that has been done - the need and grounds for remote identification of UASs has been enshrined. Without identification of the operator of the UAS, effective protection of privacy is not possible as the person liable for privacy breaches remains unknown. As the deriving legislation concerning the implementation of “U-space” (it shall implement registration, geo-awareness, and remote identification) has not yet been created, it is impossible to predict its quality and effectiveness. However, the authors believe that registration and remote identification possibilities in the use of UASs are essential and shall make a huge contribution to the effectiveness of privacy protection. However, it should be noted that the requirement for remote identification is not applied to all types of UASs. By imposing an obligation to make sure that each operator of UAS equipped with a video recorder is registered, a declarative tribute to privacy is given. Furthermore, an exception to the requirement of remote identification is made for UASs considered as toys and C4 class UASs. Therefore the provisions of Regulation 2019/947 presuppose an idea that remote identification is for assurance of physical safety

(aircraft of class C4 are allowed to be conducted in the 'open' flight category which sets minimum requirements for the conduction of flights and does not require to have remote identification function only because of „the good level of safety achieved" (European Commission 2019b), whereas registration of operators serves for privacy protection (obligation for the operators to register themselves if they operate UASs equipped with a sensor able to capture personal data (European Commission 2019b). However, the authors believe that precisely the requirement that UASs were equipped with remote identification add-ons serves best for privacy protection. Therefore the requirement for all UASs to have remote identification add-ons must be set as remote identification add-on is the main technical tool allowing effective assurance of privacy protection in the use of UASs. The only possible exception could be made for toy models of UASs only because of the principle of proportionality (to avoid disproportionate requirements that would harm economic and social interests). However, as the toy models can also carry a camera and collect information on private life, the rule requiring for a pilot of a toy model to stay at the visual line of the UAS and be identifiable (for example, he/she should wear a bright-coloured vest) must be set.

The authors hold that the exceptions to the obligation for UASs to have remote identification add-ons provide a basis for abuse, as the UAS pilot having an intention to gather information on a private life may use UAS for such illegal purpose easily avoiding identification and, accordingly, liability for illegal actions. This is because the operator cannot be identified and because of another reason: if the law enforcing bodies in the future would have the right to neutralise UASs being operated illegally, it could be quite problematic from a distance to distinguish whether the UAS in operation is the one falling within the exception of the requirement of remote identification add-on or whether the UAS is being used in violation of legal requirements. Regulation 2019/947 states that lower requirements for class C4 aircraft are introduced for the reason that such type of an aircraft has achieved a good level of safety and is comparatively simpler than other classes of unmanned aircraft, therefore, higher requirements would be disproportionate (European Commission 2019b). However, such a legislator's attitude is open to criticism because it should focus not only on the physical safety of the operations of UASs but also on privacy protection the effectiveness of which is currently questionable.

Even though Regulation 2019/947 mentions overflight of uninvolved persons, residential areas, assemblies of people as criteria worth considering on UAS flights, it is obvious that the criteria are also associated with flight safety, but not the protection of privacy. Therefore it is

worth considering including in national legislation private home areas as the areas above which UAS operation has additional restrictions (for example, permission to cross the home territory only if unavoidable, but not repetitive overfly or continuous flying above the territory).

Furthermore, besides the suggested rules, the law enforcement agencies' right to neutralise the UASs in case of the breach of the requirements for identification should be enshrined. However, technical ways and possibilities for the neutralisation of the illegally used UASs are the topics of other, technical, sciences but the legal grounds of effective enforcement of such rules must be set. To avoid possible disputes concerning such actions, the rules for the enforcement agencies' right to neutralise UASs should be short and clear, determining precise indications of the existence of the infringement. For example, if it was impossible to remotely identify the UAS and its operator is not in a visual line from the UAS (or is not recognisable) – these should be the conditions allowing to neutralise the UAS without any further investigation (presuming that the requirements of being identifiable for operators of toy models are set).

When responsible for the UAS operation person is determined, another very important step in the application of liability for the privacy-related breaches is evidence preservation. As, for example, criminal liability requires proof of the offender's fault - intention to gather private information (even direct intention must be proved).[5] Thus, without the recorded material it is impossible to prove this element of liability. Timely acting in evidence preservation is essential for privacy protection to be effective. For this purpose, it is necessary to empower the competent authority to preserve the evidence at the scene of the event (especially having in mind that remote identification add-ons shall be able to transfer information on the geographical position of the remote pilot or, if not available, the take-off point) (European Commission 2019a), as later evidence preservation would be impossible because the UAS pilot would simply hide, destroy or deny the existence of the video record. The content of the video would normally be the main evidence in civil and criminal proceedings allowing the court to decide whether the UAS pilot just flew the UAS over the private home area or was observing it intentionally.

[5] „A person shall be punishable for commission of a crime or misdemeanour through negligence solely in the cases provided for separately in the Special Part of this Code" (Criminal Code of the Republic of Lithuania 2000); see also *S.B.,V.B., R.B.* [2011] PK-72-635/2011.

CONCLUSIONS

The most important thing for privacy protection in the use of UASs is the possibility to identify the operator of the UASs which enables the responsible institutions or injured party to claim for the responsibility of the fault person.

The new legislation at the EU level, Regulations 2019/945 and 2019/947, establish the tool of identification of UASs and oblige that particular types of UASs were equipped with remote identification add-ons. Even though the wording of such obligation presupposes that such obligation is to ensure the safety of the operation of UAS (because the reason why UASs of C4 class are not required to be equipped with such add-on as is, according to the legislator, that UASs of class C4 are simpler than other classes of UASs and they have achieved the good level of safety) but it also serves for the protection of privacy.

The Regulation 2019/947 enshrines obligation for the operators to register themselves if they operate UASs equipped with a sensor able to capture personal data which is a measure dedicated precisely for the protection of privacy. However, it seems that this measure is only declarative but not practically effective as it is doubtful that an operator willing to illegally collect private information will register himself/herself, whereas operating the type of UAS which is not required to be equipped with remote identification add-on, would enable secret surveillance of privacy subject without the possibility to identify the operator of the UAS. In other words, the exceptions open the possibility of abuse, also, aggravates the work of responsible institutions as it would be difficult from a distance to determine if a particular UASs, flying without remote identification add-on is the one, which falls under the exception of the requirement to be equipped with the add-on, or not. For this reason, in the authors' opinion, the requirement of remote identification add-ons should apply to all types of UASs, except for toys models. However, the operation of toy models of UASs should be allowed only in open areas where the UAS's operator would be in a visible line from the UASs and should be identifiable by, for example, a bright-coloured west, bright ligaments, etc. If it is impossible to remotely identify the operating UAS and its operator is not visible, the right of responsible institutions to neutralise such UAS should be enshrined in the legislation.

Evidence preservation is another important aspect concerning privacy protection in the use of UASs which should be considered when applying the Regulations. As the identification of the operator of UAS is not sufficient to claim for the responsibility of him/her. Without

preserving the records made by a camera mounted on the UAS, proving the intentional fault of the operator would be impossible.

REFERENCES

1. Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and third-country operators of unmanned aircraft systems, *OJ L 152, 11.6.2019, p. 1–40.*
2. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, *OJ L 152, 11.6.2019, p. 45–71.*
3. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys. OJ L 170, 30.6.2009, p. 1.
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–88.*
5. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.), *OJ L 212, 22.8.2018, p. 1–122.*
6. The Law Supplementing the Constitution of the Republic of Lithuania with the Constitutional Act 'On Membership of the Republic of Lithuania in the European Union' and Supplementing Article 150 of the Constitution of the Republic of Lithuania (no. IX-2343) of 13 July 2004, Official Gazette (2004, no. 111-4123).
7. Lietuvos Respublikos baudžiamasis kodeksas (Criminal Code of the Republic of Lithuania). Official Gazette, 2000, No. 89-2741.
8. Bepiločių orlaivių naudojimo taisyklės (The rules for the use of unmanned aircraft). TAR, 2014, No. 2014-00438.
9. Judgement of 17 January 2008 of the Constitutional Court in the Case No. 2007-11-03, para. 25.4. Latvijas Vēstnesis. 2008, No. 12.
10. *S.B., V.B., R.B.* Ruling of Taurage District Court, 2011, No. PK-72-635/2011.
11. Kokott, J., Sobotta, Ch. (2013). 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,' *International Data Privacy Law,* Vol. 3, No. 4: 223.
12. Mikelsone, G. (2013). 'The Binding Force of the Case Law of the Court of Justice of the European Union,' *Jurisprudence,* 20(2), p. 469–495.
13. Pūraitė, A., Bereikienė, D., Šilinskė, N. (2017). 'Regulation of Unmanned Aerial Systems and Related Privacy Issues in Lithuania.' *Baltic Journal of Law & Politics,* 10:2, 107-132.