DRONES, PRIVACY AND DATA PROTECTION

Andrei-Alexandru STOICA*

Abstract

Data protection in the robotics and drone age must be included for an overhaul as technology evolves and offers new ways that could make current laws obsolete.

This paper focuses on showcasing weak points in data protection laws that are generally seen in states such as the ones that comprise the European Union or in the United States of America, which could also be seen in other states, while also analyzing some solutions that have been implemented. To identify the key issues, the paper will take into account major incidents that took place regarding breaches of data privacy, while also trying to distinguish how international law is applicable.

Drones come equipped with different types of equipment that must comply with different sets of rules and regulations, but can hardware alone prevent breaches of data protection or should operators and manufacturers be liable for these breaches? Furthermore, the issue at hand should also be covered with regards to a growing segment of drones that come equipped with artificial intelligence.

Notwithstanding, the paper will analyze if counter-drone systems could help mitigate data protection breaches or rather if they generate an extra issue that lawmakers and manufacturers have to handle.

Keywords: *drones, privacy, international law, European law, comparative analysis.*

1. Introduction

The notion of a drone is a more colocvial termn that describes unmanned vehicles. This termn is widely used to describe any type of unmanned vehicle but the most common types are those outfitted with rotary engines on either quad-propeller based platforms or fixed wings.

This paper will focus mostly on the aerial type of unmmaned vehicles since these are the most commercially available for the general population.

The author acknowledges that camera and audio drones do exist that are based on a wheeled or continuous track, but those are used only in a controlled environment and are yet to be fully accessible to the general population and governmental agencies.

As such, a "*drone*" as a termn is used to describe any aircraft without an on-board pilot. But that is an oversimplification that masks the incredible range in shapes, sizes and capabilities that characterize today's unmanned aircraft.

Another aspect towards identifying a drone as an unmanned vehicle is that it's different than a model airplane/vehicle and a toy.

For this reason, models are largely flown within visual line of sight and in the presence of an operator who watches and maintains control of the airplane during flight. That alone is enough to place model airplanes cleanly outside the boundaries of "*drone*."[1]

The drones that currently have the biggest impact on privacy are the cam-drones since they can record audio, videos and can store both locally and on the cloud.

2. The usage of drones and privacy concerns

Drones or unmanned vehicles have seen their usage grow ever since the 20th Century, when unmanned aerial vehicles were used by the U.S. Army for training purposes and as an experimental straight line rocket[2]. One of the closest equivalent of today's drones would have been the Goliath tracked mine[3] , a small wired controlled tracked vehicle capable of delivering explosives from a long range, but while its idea was revolutionary, the fact that it had a wired connection to the operator meant that it could be easily cut off from commands and rendered inoperable.

Later on, drones got equipped with cameras for spying and got used extensively during the Cold War period to spy on nuclear programs[4]. These drones became a norm in surveillance technology that allowed armies to have eyes on objectives without putting a human in harm's way.

The spy drones were often used against known targets and potential targets, meaning that the unmanned drones were used over the territory of foreign states and captured footage of key locations (military, economy or research). Unfortunately, programs that used drones, such as the US D-21[5] drone information that was declassified with the Freedom of

* PhD. Candidate at the Faculty of Law, "Nicolae Titulescu" University (e-mail: stoica.andrei.alexandru@gmail.com).

[1] John Villasenor, What is a drone, anyaway?, Scientific American, 12.04.2012.

[2] Chelsea Leu, The secret history of World War II-Era drones, Wired, 16.12.2015.

[3] Military History Matters, Back to the drawing board – The Goliath tracked mine, Military-History.org, 12.07.2012.

[4] David Axe, The Mach 3 D-21 drone was a secret America Cold War spy machine, Nationalinterest.org, 7.11.2019.

[5] See note 3.

Information Act[6], were terminated very early after a few runs because the drones were hard to recover once launched and could fall into a foreign state's influence.

As an answer to the constant threat of foreign spying, the Treaty on Open Skies[7] was adopted to give all parties a direct and legal way of gathering information about military forces and activities with an open surveillance so that it will lower tensions and possibility of military escalation.

Moving towards a civilian usage of unmanned vehicles, drones have begun being a frequent sighting at special events and public gatherings, being used mainly by event organizers, activists or law enforcement agencies.

What this paper will focus on is how privacy is being handled by civilian drones and whether drones equipped with cameras must be handled in the same way as CCTV. Most states inside the Union and outside of it have already accepted that they must comply with the European Union's General Data Protection Regulation[8] for how they handle activities on the internet, but seeing as how the European Union will implement Regulation 947/2019[9] (which deals with the rules and procedures for the use of unmanned aircraft by pilots and operators, defining categories of use and a series of requirements for their use) and Regulation 945/2019[10] (which deals with the requirements of unmanned aircraft systems and the requirements to be met by designers, manufacturers, importers and distributors in order to obtain conformity markings and monitor the market for safety and interest in the competitiveness of it), manufacturers and users must learn to comply with how they handle with how data is being gathered and used by and from the drone.

While these may act as a code of conduit for European states, the latter Regulation is addressed towards third party states who would want to bring drones inside an E.U. state and could contribute towards a global mechanism to protect privacy and data. The most common regulations that cam-drones must follow are those that are similar to surveillance cameras.

The issues that arises from usage of drones can lead to violations of privacy and data protection laws. For example, the U.K. Royal Mail started in December 2020 a delivery program with drones towards remote regions[11] that will expand over time in similar fashion to the U.S. counter-part delivery system where a waiver was allowed by the national administration for drone delivery systems over houses[12].

The aforementioned situations can be seen as a blessing in disguise, mainly because it will allow faster deliveries, but will also raise the issue of how the information that the drone is gathering directly or indirectly when it will fly over a person or building.

Most current drone flights are handled by militaries, law enforcement agencies, and border agencies and have started being used in energy and agriculture infrastructure, but the former fall under a legal waiver where the drones can be handled under certain scenarios, while the latter fall under scenarios where they are used in remote regions where privacy and data protection are not a big issue.

However, one of the fundamental human rights found in the Universal Declaration of Human Rights[13] reads that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." As such, drone flights must be handled in such a way that any intrusion can be blocked or prevented.

Seeing as how the United States of America has had a lot of issues with aerial surveillance and because its law system allows the judicial precedence, it will offer an interesting insight in how drones and their operators can fail to uphold other people's rights.

In the judicial practice of the U.S.A., the most resonating cases regarding privacy breaches in different situations that required or not a warrant are *California vs. Ciraolo*[14], *Katz vs. U.S.*[15] and *Smith vs. Maryland*[16].

To put the cases into context, the Ciraolo case is the most definitive since it involved the use of a police helicopter to do an aerial observation of a person's backyard without warrant, while the images had been used to successfully convict the person. The ruling was later appealed and it was found that the images were taken without a warrant and as such were in violation of the U.S. Constitution.

The ruling stated[17]:"On the record here, respondent's expectation of privacy from all observations of his backyard was unreasonable. That the backyard and its crop were within the "curtilage" of respondent's home did not itself bar all police observation. The mere fact that an individual has taken measures to restrict some views of his activities does

[6] National Reconnaisance Office, USA, information for the how to access information with the FOIA https://www.nro.gov/Freedom-of-Information-Act-FOIA/Declassified-Records/Special-Collections/D-21/.

[7] Entered into force on 01.01.2002, has 34 party states. As of November 2020 the U.S.A. withdrew from the treaty.

[8] Regulation 679/2016 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).

[9] Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

[10] Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

[11] Charlotte Ryan, Royal Mail brings Scottish Isle closer with drone, Bloomberg, 16.12.2020.

[12] Miriam McNabb, DroneUp's waiver for flight over people is a major step for drone delivery, Dronelife.com, 07.12.2020.

[13] Adopted by the U.N.G.A. in 1948, Resolution 217A, article 12.

[14] U.S. Supreme Court, 476 US 207, 1986.

[15] U.S. Supreme Court, 389 US 347, 1967.

[16] U.S. Supreme Court, 442 US 735, 1979.

[17] See note 13, pg. 208-215.

not preclude an officer's observation from a public vantage point where he has a right to be and which renders the activities clearly visible. The police observations here took place within public navigable airspace, in a physically nonintrusive manner.

The police were able to observe the plants readily discernible to the naked eye as marijuana, and it was irrelevant that the observation from the airplane was directed at identifying the plants and that the officers were trained to recognize marijuana. Any member of the public flying in this airspace who cared to glance down could have seen everything that the officers observed. The Fourth Amendment simply does not require police traveling in the public airways at 1,000 feet to obtain a warrant in order to observe what is visible to the naked eye."

The other two cases argued that a warrant is also required when analyzing and intercepting a phone call in public space and inside a person's home. This roughly translates to a requirement that a drone operator has to not use the drone to spy and record people without their consent.

Similar to the Ciraolo case, *Florida vs. Riley*[18] featured a manned aerial vehicle that was used for aerial observation of a greenhouse, while maintaining around 120 meters altitude. The Court established that it was no violation of his property and privacy laws since the greenhouse was constructed in such a way as to promote the idea that it was trying to maintain intimacy. Such a case argues that a drone operator must take into account that processing information gathered by the drone must be censored upon public release, but only if the object or person that was filmed or photographed was even indirectly not doing something to protect the privacy of himself or the property.

In another landmark case, *Dow Chemical vs. U.S.*[19] it was argued that aerial photographs using a "*standard precision aerial mapping camera*" to conduct an investigation under the Clean Air Act can be handled without a warrant if it's in navigable space. The Court also argues that even though there are fewer concerns about privacy in the context of an industrial plant than with respect to a home, intrusion by certain technology unavailable to the public may be prohibited by the US Constitution.

All of these cases highlight that privacy is a very important aspect when flying over someone's property, mostly because the person who may feel that his or her rights are being encroached can even resort to using armed force against the drone. In the case of *Boggs vs. Mereideth*[20] a person shot his neighbors drone that was midair because he felt that the drone was violating his houses airspace.

The case was dismissed on jurisdictional claims, seeing as how the airspace is being handled by the Federal Aviation Administration and it was seen as an anticipated defense derived from federal law.

While the case offers a lot of space for theory crafting, the federal government issued in December 2020 a new Rule[21] entitled Remote ID and it states that*: "Under the final rule, all UA required to register must remotely identify, and operators have three options (described below) to satisfy this requirement. For UA weighing 0.55 lbs or less, remote identification is only required if the UA is operated under rules that require registration, such as part 107".* This new addendum to the existing legislative actions have brought a new ability for operators, that is the ability to fly over people and moving vehicles varies depending on the level of risk a small drone operation presents to people on the ground, both during the day and night.

The final rule requires that small drone operators have their remote pilot certificate and identification in their physical possession when operating, ready to present to authorities if needed. This rule also expands the class of authorities who may request these forms from a remote pilot. The final rule replaces the requirement to complete a recurrent test every 24 calendar months with the requirement to complete updated recurrent training that includes operating at night in identified subject areas.

As for privacy fears, the federal body acknowledges that privacy issues could be a concern with operations over people; however, the proposed performance-based rule focuses on the risk of injury involved with operations over people and does not address privacy issues. They also stated people over whom a small unmanned aircraft flies should receive advance warning, both at public events and in closed or restricted-access sites.

This new ability offered to registered operators could lead to unwanted spying of public events or even illicit third party monitoring of police investigations, to name a few. Sadly, the F.A.A. emphasizes that privacy issues are outside the focus and scope of the rule, however, this rule does not relieve the operator from complying with other laws or regulations that are applicable to the purposes for which the operator is using the small UAS. Drone manufacturers will have 18 months from the moment the Rule was brought to public attention to begin producing drones with remote identification.

The new federal rule brings more issues than it solves, since home owners will try and use different anti-drone technology, which could potentially affect its controls or GPS and crash said drone, causing damage or even harm.

[18] U.S. Supreme Court, 488 US 445, 1989.
[19] U.S. Supreme Court, 476 US 227, 1986.
[20] Debra Cassens Weiss, Does property owner have the right to shoot down hobbyist's hovering drone?, AMERICAN BAR ASSOCIATION JOURNAL, 14.01.2016.
[21] Part 89 issued by the F.A.A., 28.12.2020. The executive summary can be accessed at the following: https://www.faa.gov/news/media/attachments/RemoteID_Executive_Summary.pdf.

The general reaction (regardless of legal system of the state) is that attacking a drone is the equivalent of attacking someone's property, but this is also available for the drone operator as well since he is liable of civil and/or criminal charges (for example trespassing). Compliance with the data protection requires, among other things, that you only gather and use footage fairly and lawfully.

The best solution is to notify the law enforcement agencies, while states must begin drafting no-drone-zones and adopt special law enforcement policies to counter illicit drone actions.

In Europe, the situation is fairly more straightforward, because member states of the European Union and the Council of Europe must comply with Regulation 679/2016 and Treaty no. 108[22], while also have to follow the European Convention on Human Rights and its understanding of private life and property.

In the view of the European Court of Human Rights, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life[23].

The European Union later adopted Directive 2016/680[24] for protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data, and it establishes data protection principles applicable to the processing of personal data in the area of justice, such as fair and lawful processing, proportionality, accuracy, limited conservation time, and responsibility.

Thus, the European legislation is applicable to police drones as well, meaning that justice authorities can have drone footage challenged and even annulled if it was gathered in an illicit manner, while also having to store, handle and delete certain data that was gathered with drones. The same could be applied to situations in other states as well.

However, seeing as how drones are unmanned vehicles but are treated as manned and operated vehicles, it should be noted that they should comply with aviation rules guaranteeing the total aviation safety system and consequently they must be approved by a competent authority, the operator shall have a valid RPAS operator certificate, the remote pilot must hold a valid license[25].

The future of drones was set-up through the Riga Declaration on Remotely Piloted Aircraft[26] with a progressive-risk-based task for regulation of drones, meaning that public acceptance of drones has to be handled with key aspects such as public authorities implementing ways to handle illicit drone handling, geospoofing, cyber security and implementing no-fly zones. To design such a legal and administrative system, the F.A.A. and E.A.S.A. have established a somewhat common regulation[27], both of them having fairly similar rules regarding weight limitations, flight periods and locations, and most importantly, airworthiness certifications for both the drone and its pilot.

To allow them to be operated, drones are normally combined with applications such as cameras or video-cameras (as the remote pilot has to see or detect what is in front of the drone to avoid a collision). They might also record the images, through software to process the video images, which might have further applications. For example, the U.S.A. has developed a mobile phone app entitled B4UFLY[28] that informs the user of no-fly zones (permanent or temporal) and even has a legislation option, so that the user can learn the rules on the go.

Other developers-manufacturers, such as DJI[29], have preinstalled a safety software inside their drones to warn the user of flying over sensitive locations and that in certain areas the user has to upload a special clearance permit or even pass an examination.

This has also become a norm for operators since the U.S.A. have implemented Remote ID, with the E.U. and U.K. implementing Drone Remote Identification Protocol (DRIP)[30] that will enable confidential handling of private information and all information designated by neither cognizant authority nor the information owner as public. It will also, enable selective strong encryption of private data in motion in such a manner that only authorized actors can recover it. If transport is via IP, then encryption must be end-to-end, at or above the IP layer, while notwithstanding it enables selective strong encryption of private data at

[22] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1985.
[23] Uzun vs. Germany, E.C.H.R., Application no. 35623/05, 02.09.2010, paragraph 52.
[24] *OJ L 119, 4.5.2016, p. 89–131.*
[25] Ottavio Marzochi, Privacy and Data Protection Implications of the Civil Use of Drones, European Parliament, Directorate General For Internal Policies, PE 519.221, June 2015, p. 13.
[26] RIGA Declaration On Remotely Piloted Aircraft (Drones) "FRAMING THE FUTURE OF AVIATION" Riga - 6 March 2015.
[27] For reference the F.A.A.'s regulation for small drones is Part 107, and the E.A.S.A.'s equivalent is the EU Regulation 2019/947 and 2019/945.
[28] Link for description and download https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/b4ufly/.
[29] Link for the features of the integrated software https://www.dji.com/flysafe/introduction.
[30] S. Card, Ed., A. Wiethuechter, R. Moskowitz, Drone Remote Identification Protocol (DRIP) Requirements, Ietf.org, 19.11.2020.

rest in such a manner that only authorized actors can recover it.

While the U.S.A. has case laws regarding flight of manned vehicles over properties and its repercussions on privacy, Europe has the benefit of having a better legal safeguard mechanism in the scope of the European Court of Justice and the European Court of Human Rights. This means that under the privacy and private life guarantees offered by these mechanisms.

As such, the E.C.J. case *Rynes vs. Úřad pro ochranu osobních údajů*[31] retained that the application of the right to privacy and data protection to private and public spaces, which implies that EU law applies regardless of the location of the person contesting the dronerelated interference. It also stated in a preliminary ruling related to CCTV that the "*household exception*" does not apply when the personal data is gathered in public spaces.

Also, should such data be shared trough a social network or published on the internet, the exception would not be applicable and the full guarantees provided by the Directive would apply. Furthermore, it is likely that the capturing and processing of personal data carried out by drones in public spaces would not be covered by the "household exemption" and hence such processing would be subject to data protection law.

However, the most common exception to data protection and privacy of drones will remain that of intelligence services, who fall outside of the E.U. competences, including when these imply the collection of data through drones.

Another issue, that legislation does not address, is the fact due to their size, drones can collect data without being recognized and therefore individuals who are being watched or monitored are not aware of this and can not only collect personal data such as videos with or without sound but also transfer the gathered data at the same time as the subject is being watched.

A more dystopian view on the usage of drones was brought up as a possible data protection risk that is the so called ”*profiling*” of personal data[32]. This can roughly mean that a drone can be used for marketing purposes, identifying customers based on their previous purchases.

Moreover, selling companies could use the sold drone, loaded with video-cameras, GPS and face recognition for tracking and identifying their existing and potential customers based on the cars they drive and their addresses, in order to perform targeted advertising. This information could later be sold, traded or transferred in a similar matter to how Google Adware or Facebook uses its information gathered with their algorithms.

Article 8 of the European Convention of Human Rights includes the notion of personal data, this being outlined in the case *S. and Marper v. U.K.*[33] personal data is linked with the right to respect for private and family life are guaranteed by article 8 of the Convention.

As such, states must ensure that personal data is not easily accessible by unauthorized third parties. This means that states must ensure that a household exception can be applied, when private individuals perform personal and family life related activities and that if the data collected is then shared or uploaded on online platforms via the internet, this exception cannot be applied and the rules provided by data protection laws have to be followed.

In the case of drones, operators must be aware that they are not covered by the household exception when they use the drone in public spaces for leisure or hobby activities. If such activities are performed on private property then the household exception is applicable, but it has limitations depending on where it is used or at what altitude. The maximum allowed altitude for leisure/hobby flights is around 400 feet or approximately 120 meters[34].

Furthermore, based on the G.D.P.R., drones must be developed and manufactured with data protection as a core design choice, meaning that manufacturers develop the hardware and software, but the operator is responsible for the way the drone was used.

These specifications that fall under the guidelines for manufacturers, are meant to provide a minimum standard of data protection, which would make the drone industry fall in line with the new regulation and therefore respect privacy and data protection rights of individuals, at least from hardware and software perspective.

The second aspect that drones may have already preinstalled, is that data protection as a default setting thanks to legislative guidelines, but as it stands it fails from a real time sharing aspect, meaning that streaming services from outside of the state where the drone is being handled may require a third party data protection mechanism for protection.

Notwithstanding, in public places, individual privacy is similar to the concept of non-privacy because by entering a public place and remaining there, there is an implication that one is aware they will be seen or recognized, and that one’s behavior may be scrutinized by anyone in that public sphere who may draw inferences from the individual’s behavior[35], meaning that drone operators must apply the *„reasonable expectation of privacy”*[36] where private life

[31] Case C-212/13, 11.12.2014.
[32] Florin Costinel Dima, Drone technology and human rights, University of Twente, 6.07.2017, p. 27-28.
[33] European Court of Human Rights, 30562/04 and 30566/04, 4.12.2008, para. 68-69.
[34] Airmap, The rules you need to know to fly recreational drones, Airmap.com, updated as of 23.07.2019.
[35] European Court of Human Rights, Costello-Robers vs. U.K., 89/1991/341/414, 23.02.1993, para. 35-36.
[36] As seen in the E.C.H.R. in the case of P.G. and J.H. vs. U.K., 44787/98, 25.09.2001.

considerations may arise once a systematic or permanent record of material from the public domain comes into existence.

The most important aspect of data protection introduced by the European Union G.D.P.R. is forbidding automated decision making. Under article 22 of the G.D.P.R.[37], consent is needed when decisions are solely automated and have a legal or similarly significant effect on people and if such automated decision making is not authorized by law. This means that information gathered or generated by drones must be filtered by the operator in such a way that it cannot be shared without consent or without a human review and validation.

In 2019 the U.K. police used an automated facial recognition software in public space and caused an uproar because of it was not clear who can be placed on the watch list, nor was it clear that there are any criteria for determining where the cameras could be deployed[38]. The system was challenged in the case of *R vs. CC South Wales*[39] where the Court ruled that *"too much discretion is currently left to individual police officers"* and the Court also held that the police did not sufficiently investigate if the software in use exhibited race or gender bias.

Such a case argues how easily drones can be placed in public space and cause a privacy problem in which the operator could never be found to be held responsible.

However, the Amsterdam Drone Declaration[40] established a focus on local needs and initiatives and a push towards integrated smart mobility and fair access to all dimensions of public space.

Smart mobility under data protection must be understood as a set of guidelines that any drone operator should know and abide. For example, the U.K.'s independent authority for data protection, the ICO[41], outlined that operators should let others know before they start recording, and also should keep the data in a safe space inside the drone.

While these outlines are general and beneficial to any type of drone operator, the fact that drones have a tendency to malfunction due to hardware or software issues or have accidents due to human errors leads to another possible type of data protection breach.

Civilian drone incidents have been documented by mass-media[42] where drones have crashed on the White House lawn or collided with a small manned aircraft at Quebec's airport. These incidents raised issues where the operator should have been prosecuted, but not all cases can be resolved since not operators are licensed or have their drones registered.

These cases can also lead to the drones being recovered by third parties who may extract the information stored on the drone, information that was not yet filtered by the operator and as such could spell a breach in a person or a company's private data. This also works both ways, since[43] other incidents such as trafficking drugs or terrorism conducted with drones could be intercepted in a way to deter potential high risk crimes.

As such, modern problems require modern solutions.

3. Possible solutions for protecting data and privacy

Solutions vary based on how local administrations and governmental agencies are able to handle and intervene to prevent drones from breaching property and privacy laws.

The most common and useful solution is to declare zone as no-fly zones and as such limit drone access to the designated areas and sanction those who do not commit to respecting said regulations.

For example, the United Kingdom[44] established no-fly zones designated as *danger areas* where it is often used for activities such as fighter pilot training, live ammunition training or weapons and systems testing (including GPS jamming exercises). Other zones are designated as *prohibited* or *restricted* and are clearly established by the air administrative authority. What is important is that person who are interested can request that their property or business area be declared as unsafe spaces for drone flights.

---

[37] Article 22 contents:"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;
(c) or is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

[38] Kate Cox, Police use of facial recognition violates human rights, UK court rules, ArsTechnica, 8.12.2020.

[39] EWCA Civ 1058 C1/2019/2670.

[40] E.A.S.A., Drone Declaration, Amsterdam, 28.11.2018.

[41] Information Commissioner's Office, Your data matters – drones - https://ico.org.uk/your-data-matters/drones/.

[42] Igor Kuksov, Air alert: 8 dangerous drone incidents, Kaspkersky.com, 21.10.2019.

[43] Worldwide drone incidents charted by Dedrone.com, accessible at https://www.dedrone.com/resources/incidents/all.

[44] Applying UK Air Navigation Order CAP393, no fly zones as of 01.01.2021: https://www.noflydrones.co.uk/.

Usually, the air space regulations prohibit drones from flying close to airports, large cities, sensitive industrial sites, nuclear facilities, military bases, prisons and natural reserves.

Administrations can temporary declare no-fly zones[45] while a special event or holiday is being played out. For example, France declared that the area designated for the *Tour de France* be considered a no-fly zone during the event.

In Europe, Eurocontrol[46] allows drone users who are interested in operating their unmanned aerial vehicle on the territory of another state to check the guidelines for safety and no-fly zones via an online tool that showcases 19 states who have submitted updated information in this regard.

From an international point of view, third parties have developed internet tools[47] that follow the I.C.A.O. guidelines, the U.S. F.A.A. guidelines and other states aerial recommendations. The tools allow interested parties to check free use zones and prohibited zones in almost any state around the world, but they must also check with the state they want to fly in or transit with the drone for temporary modifications or drone type bans.

Other solutions to prevent privacy invasions may come in the form of anti-drone devices or systems.

Broadly speaking, counter-drone systems are either fixed on the ground, mobile on a ground vehicle, hand-held by a single person, or mounted on another drone.

Finding a drone by either radar or radio frequencies can be done and such devices are accessible to the general population, but other types of anti-drone systems may be out of reach or illegal. Such devices may include GPS spoofers, anti-drone ammunition, radio jamming, lasers, microwave rays or even kamikaze drones.

For the most part, counter-drone systems are expensive, out of reach of almost all people, most businesses, and some governments. Securing the skies against the possibility of a threat must be weighed against the cost of acquiring and then using the system and as such care must be taken to make sure that the drones targeted pose a threat and are not just errant hobbyists unaware that they are piloting their toy into contested skies[48].

Also, counter-drone systems may cause other collateral damage to authorized users, meaning that for example a radio jammer or GPS spoofing technique could unintentionally interrupt communications of other small airplanes or helicopters or even other drones. This could be interpreted as a criminal conduct regarding laws that prohibits willful or malicious interference to communications.

In the U.S.A., the aviation authority stated in 2016[49] that: „Unauthorized UAS detection and counter measure deployments can create a host of problems, such as electromagnetic and Radio Frequency (RF) interference affecting safety of flight and air traffic management issues. Additionally, current law may impose barriers to the evaluation and deployment of certain unmanned aircraft detection and mitigation technical capabilities by most federal agencies, as well as state and local entities and private individuals. There are a number of federal laws to consider, including those that prohibit destruction or endangerment of aircraft and others that restrict or prohibit electronic surveillance, including the collection, recording or decoding of signaling information and the interception of electronic communications content.”.

Later, the federal aviation authority from the U.S. did a follow-up study in 2018[50] concluded that drone detection systems should be developed so they do not adversely impact or interfere with safe airport operations, air traffic control and other air navigation services, or the safe and efficient operation of the national air service. Also, the study showed that the costs of having a permanent counter-drone system is very high and could become obsolete by the time it’s installed and operational.

Most legislative actions in the U.S. will however be reviewed after 31st of December 2022 when the modernization of law enforcement agencies and military structures will probably end and it will allow a more commercialized defense mechanism to be accessible to the general population[51].

A more current solution is being handled in India with the *Digital Sky*[52] platform that will allow only those drones that comply with the no-fly and no-take-off protocols. These protocols have to be implemented software-wise by the manufacturers and will allow drones to operate in areas demarcated as green and yellow zones, permitting them to fly over most of India.

This means that for green and yellow zones, operators will get automatic clearance from the platform and for red demarcated zones, the security agencies will receive specific clearance request. All data and information is uploaded to the Digital Sky platform so that there is no scope for arguments to the contrary at a later stage.

The platform will also permit state agencies to identify and intercept the drone and to bring the alleged

[45] For example France’s temporary no fly zones: https://dronerules.eu/ro/recreational/news/france-new-map-with-no-fly-zones-and-maximum-altitudes-for-recreational-drones.

[46] A link to the online tool that offers said information: https://www.eurocontrol.int/tool/uas-no-fly-areas-directory-information-resources.

[47] ICAO no fly zones drone world website.
https://www.arcgis.com/apps/webappviewer/index.html?id=9e674cbad86f4f8c86d1854dec6a5fb5.

[48] Kelsey Atherton, Anti-drone tech’s tangled regulatory landscape, Brookings.edu, 02.10.2020.

[49] F.A.A. letter to the Office of Airports Safety and Standards in the Department of Transportation, 26.10.2016.

[50] F.A.A. letter to the Office of Airports Safety and Standards in the Department of Transportation, 19.07.2018.

[51] Jonathan Rupprecht, 7 big problems with counter drone technology, jrupprectlaw.com, 5.01.2021.

[52] *Piyush Gupta, Anti*-drone technology – a ‘simple’ answer?, Roboticslawjournal, 12.10.2020.

offender to justice can be left to the discretion of the judiciary.

Analyzing how the counter-drone strategy is being handled in most states where drones play a big part in the economy, it can be concluded that currently only law enforcement agencies (to some extent) and military operators are allowed to use anti-drone systems.

For example, the U.S.A. has adopted a Memorandum Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems[53]. Under these guidelines agencies will adopt protective measures necessary to mitigate credible threats from unmanned aircraft or unmanned aircraft systems to the safety or security of covered facilities or assets.

Agencies who are interested in obtaining clearance to use counter-drone systems then a request will be issued to the Department of Justice. Other states can lodge requests for their own events on U.S. soil.

The memorandum also addresses privacy concerns and any clearances will only be given after consultation with the official for privacy. A component may only intercept, acquire, access, maintain, use, or disseminate communications in a manner consistent with privacy laws and cannot be issued if its sole purpose is the monitoring activities or the lawful exercise of rights.

A component should consider and be sensitive at all times to the potential impact protective measures may have on legitimate activity by unmanned aircraft and unmanned aircraft systems, including systems operated by the press. State agencies components may maintain records of communications to or from unmanned aircraft or unmanned aircraft systems intercepted or acquired under authority of data protection acts.

If a drone is caught using a counter-drone measure, then that drone is seized alongside any other systems that it was being connected to. The agencies involved can issue warnings, disrupt controls of operators and even resort to the use of force to stop the drone.

Other noteworthy defense mechanisms, which have been used to protect from unwanted drone activities were deployed in Netherlands and the U.K.[54], were in the form of hawks that could be used to hunt drones since they act in a similar fashion to other small birds, but having a hawk at home could be cumbersome for most.

4. Conclusions

Privacy and data protection concerns will remain as long as drones can be easily accessible on the market and also as long as these drones are manufactured without supervision from either a state angency or legal limits established by the state.

Having a control on the quality of drones allows a slew of other mitigating facts that can ensure that privacy and data protection fall in order and will require less intervention from military agencies or law enforcement.

Having mandatory registrations for any audio-camera drones is another way to ensure protection. This is why offering flyer-IDs[55] regardless of age is a way to protect privacy since it allows a person to have a fundamental basic on the rules of flying and data protection.

Also, adding a time valability to this ID is a futureproofing measure as to ensure that the person is always learning about legislative and administrative measures adopted.

Seeing as how basic drone flying laws are common between states, having the operator and/or flyer ID valid in other states is a measure that could develop trust in drone communities.

Basic rules for drone operators should include that if the drone is fitted with a camera or listening device, then the operator must respect other people's privacy whenever the vehicle is being used. Consent must be obtained whenever another person or property is being filmed or photographed, and if that cannot be obtained, then data laws must be applied to how the information will be distributed.

Furthermore, the operator must be clearly seen when he is out with the drone as to be easily be identified both as the operator and the drone owner. The operator must store images safely and delete anything you don't need. If the recorded images are for commercial use, than it will need to meet further specific requirements as a data controller.

While U.S. Supreme Court actions allow persons to secure their properties regarding their airspace columns, other states did not take into account updating property laws in regards to drones, and as such should update their legislative measures on how a person can obtain an administrative measure from a local or national public authority in regards to protecting their privacy and property from unwanted drone flights.

As more and more drone transportations will be green-lighted so will airspace routes be formed over private properties.

Also, legislators should craft simple, duration-based surveillance legislation that will limit the aggregate amount of time the government may surveil a specific individual. Such legislation can address the potential harm of persistent surveillance, a harm that is capable of being committed by manned and unmanned aircraft.

The most lackluster legal measure is that of responsibility of operators and enforcement measures.

[53] U.S. Attorney General, 13.04.2020.
[54] Ben Sampson, Engineers flight test hawks for drone captures, Aerospacetestinginternational.com, 10.07.2019.
[55] For refrence U.K testing for flyer ID regulation as of December 2020: https://register-drones.caa.co.uk/drone-code/getting-flyer-id.

Law enforcement angecies lack the required equipment to protect people from unwanted drone harassment.

The E.U. have more recently been conducting tests of anti-drone weapons that can be used by specialized divisions of law enforcement agencies[56], while having the European airspace agencie's approval. A similar approach had begun in U.K. with the forming of a specialized team inside the national police force that can investigate illicit use of drones[57].

Other measures should require that that technology such as geofencing and auto-redaction, may make aerial surveillance by drones more protective of privacy than human surveillance[58].

From another perspective, drone privacy violations could also translate into new types of witness evidence, but this will also translate to new procedural law provisions that have to permit such feats.

Privacy concerns were raised and had to be handled in how agencies conducted air monitoring during the Covid-19 Pandemic. For example, in the U.S.A. the F.A.A. regulations regarding drone flights do not cover data protection beyond the general rule that it must be protected[5960]. As such, data protection agencies have to adopt regulatory norms for drones and have to enforce these norms.

One such legislative action that could be applied to other states is the Californian Paparazzi Law amendment to their Civil Code[61]. This law declares that drones cannot fly above residences and invade privacy and was adopted in 2014 as a reaction to journalists invading the private life of celebrities while they were in a private environment but with walled gardens.

The journalists often employed drones to take pictures or record videos of said celebrities and this sparked a lot of outcry. The law is applicable to anyone, and can benefit from protection regardless of fame, and will protect the property, regardless of open spaces on the property.

Other mechanics that could protect the data and privacy could be represented by a killswitch built inside the drone, which could delete its storage contents if it crashed, get highjacked or sold, as to ensure that the third party does not access to sensitive information or data.

Regardless of any type of data protection measure, nothing can be enforced without proper equipment and specialized personel in the administrative authorities.

The best way to protect data and privacy can be two-fold: either create guidelines for manufacturers to insert special safety and killswitch related protocols inside the drone, thus shifting the responsibility towards the operator who has to use said protocols to their furthest extent, or the second paradigm, allowing the market to be outfitted with anti-drone technology and equipping state agencies with the required devices to both counter drones and to counter-counter-drone technologies.

Regardless of choice, a state has to adopt legislation for abuses from any side.

References

- John Villasenor, *What is a drone, anyaway?*, Scientific American, 12.04.2012;
- Chelsea Leu, The secret history of World War II-Era drones, Wired, 16.12.2015;
- Military History Matters, *Back to the drawing board – The Goliath tracked mine*, Military-History.org, 12.07.2012;
- David Axe, The Mach 3 D-21 drone was a secret America Cold War spy machine, Nationalinterest.org, 7.11.2019;
- Treaty on Open Skies – 1992;
- Regulation 679/2016 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;
- Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft;
- Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems;
- Charlotte Ryan, Royal Mail brings Scottish Isle closer with drone, Bloomberg, 16.12.2020;
- Miriam McNabb, DroneUp's waiver for flight over people is a major step for drone delivery, Dronelife.com, 07.12.2020;
- Universal Declaration of Human Rights – 1948;
- U.S. Supreme Court, 476 US 207, 1986;
- U.S. Supreme Court, 389 US 347, 1967;
- U.S. Supreme Court, 442 US 735, 1979;
- U.S. Supreme Court, 488 US 445, 1989;
- U.S. Supreme Court, 476 US 227, 1986;

[56] Samuel Stolton, EU police forces to employ anti-drone guns "illegal" in the US, euractiv.com, 26.05.2020.
[57] National Police Chief's Council, DAC Lucy D'Orsi discusses criminal use of drones, npcc.police.uk, January 2019.
[58] Gregory McNeal, Drones and aerial surveillance: Considerations for legislatures, Brookings.edu, Report, November 2014.
[59] Ann Thompson, As drones become more common, privacy concern arise, Wvxu.org, 12.10.2020.
[60] Chaim Gartenberg, Social-distancing detecting "pandemic drones" dumped over privacy concerns, TheVerge, 23.04.2020.
[61] Joshua Azriel, Restrictions against Press and Paparazzi in California: Analysis of Sections 1708.8 and 1708.7 of the California Civil Code, UCLA Enterntaiment Law Review, 2017.

- Debra Cassens Weiss, Does property owner have the right to shoot down hobbyist's hovering drone?, American Bar Association Journal, 14.01.2016;
- Part 89 – Federal Aviation Administration, published on 28.12.2020;
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1985;
- E.C.H.R., Application no. 35623/05, 02.09.2010;
- Directive 2016/680 for protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data;
- Ottavio Marzochi, Privacy and Data Protection Implications of the Civil Use of Drones, European Parliament, Directorate General For Internal Policies, PE 519.221, June 2015;
- Riga Declaration On Remotely Piloted Aircraft (Drones) – 6.03.2015;
- Part 107 – Federal Aviation Administration;
- S. Card, Ed., A. Wiethuechter, R. Moskowitz, *Drone Remote Identification Protocol (DRIP) Requirements*, Ietf.org, 19.11.2020;
- E.C.J., Case C-212/13, 11.12.2014;
- Florin Costinel Dima, *Drone technology and human rights*, University of Twente, 6.07.2017;
- E.C.H.R., Applications30562/04 and 30566/04, 4.12.2008;
- E.C.H.R., Application 89/1991/341/414, 23.02.1993;
- E.C.H.R., Application 44787/98, 25.09.2001;
- Kate Cox, Police use of facial recognition violates human rights, UK court rules, ArsTechnica, 8.12.2020;
- R vs. CC South Wales, EWCA Civ 1058 C1/2019/2670;
- Amsterdam Drone Declaration – 28.11.2018;
- Igor Kuksov, Air alert: 8 dangerous drone incidents, Kaspkersky.com, 21.10.2019;
- Kelsey Atherton, Anti-drone tech's tangled regulatory landscape, Brookings.edu, 02.10.2020;
- F.A.A. letter to the Office of Airports Safety and Standards in the Department of Transportation, 26.10.2016;
- F.A.A. letter to the Office of Airports Safety and Standards in the Department of Transportation, 19.07.2018;
- Jonathan Rupprecht, *7 big problems with counter drone technology*, jrupprectlaw.com, 5.01.2021;
- *Piyush Gupta*, *Anti*-drone technology – a 'simple' answer?, Roboticslawjournal, 12.10.2020;
- Memorandum Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems, U.S. Attorney General, 13.04.2020;
- Ben Sampson, *Engineers flight test hawks for drone captures*, Aerospacetestinginternational.com, 10.07.2019;
- Samuel Stolton, EU police forces to employ anti-drone guns "illegal" in the US, euractiv.com, 26.05.2020;
- National Police Chief's Council, *DAC Lucy D'Orsi discusses criminal use of drones*, npcc.police.uk, January 2019;
- Gregory McNeal, Drones and aerial surveillance: Considerations for legislatures, Brookings.edu, Report, November 2014;
- Ann Thompson, As drones become more common, privacy concern arise, Wvxu.org, 12.10.2020;
- Chaim Gartenberg, Social-distancing detecting "pandemic drones" dumped over privacy concerns, TheVerge, 23.04.2020;
- Joshua Azriel, Restrictions against Press and Paparazzi in California: Analysis of Sections 1708.8 and 1708.7 of the California Civil Code, UCLA Enterntaiment Law Review, 2017.