Adnan DURAKOVIĆ, PhD[*]
Law Faculty, University of Zenica
Full professor

Sabina DURAKOVIĆ, MSc
School of Economics and Business,
University of Sarajevo

Review Scientific Article
Received: June 8 2020
Accepted: July 1 2020
UDK: 351.814:629.7.014.9
342.721
https://doi.org/10.47152/rkkp.58.3.3

REGULATING THE NON-MILITARY USE OF DRONES AND PROTECTION OF PRIVACY

In last few years we are witnesses of strong development of drones' capacity not only for military purposes but also for civilian use, particularly for police surveillance, investigations, arrests and search and rescue operations. Up until now not even United States of America adopted unified laws considering the use of drones and their impact on privacy but it is obvious that legal, administrative and justice framework for balancing these two conflicted interests and demands will soon be developed. This article will give the review of legal problems and solutions from literature covering countries which are the leaders in this field of technology and law.

Key words: drones, privacy rights, regulations

1. Introduction

It is beyond doubt that, except for military purposes where they have proven to be effective weapons, drones seek their place in civilian use. The first future beneficiaries of civilian government institutions are the police and other similar

[*] e-mail: dadnan07@gmail.com

agencies, but pressure and lobbying to liberalize the use of drones also comes from numerous private and commercial users. The notoriety of military use of drones has led to public distrust that much cheaper and smaller aircraft than those who are more technologically advanced could be used massively by numerous civilian entities. It is true that civilian aircraft have less technological capacity, but are physically smaller and less visible, and thus easily used for universal surveillance of citizens and their privacy. The focus of the paper is to analyze two areas of application and two tracks for the legal regulation of the use of drones. The first concerns is the use of drones by police for criminal investigations and other police activities, and the second concerns is the civil (positive or negative) use of drones, which may also have criminal repercussions. The main hypothesis of the paper is that: existing legal regulations are not sufficient to cover the new technologies that drones bring along and affect the privacy and freedoms of citizens. The auxiliary (second) hypothesis is that drone regulations must take into account, in addition to technology, certain other factors that limit the ability, duration and quality of surveillance carried out by drones.

2. Legal Aspects of Using Drones

2.1. Technological specifics and preconditions for legal regulation

The drones changed the warfare because they made it easy to find and eliminate people posing security threats without endangering the lives of soldiers on the ground. Today's drones are not much different from earlier radio-controlled planes, as they do not have full autonomy, but today they are automated. This means that they can do some of the work on their own, but are generally operator dependent. Unmanned aerial vehicles will soon be able to operate independently and make decisions. Already in some countries, drones are being used to guard prisoners or provide care to patients (Marra, Mcneil, 2012: 5). Drones are specific by the technology which is drastically changing, and current legal solutions based on current technology may not be valid and effective tomorrow. Autonomy is a keyword for robots and drones and is defined most commonly from the point of view of human nature as a combination of freedom and responsibility on the basis of which it operates, as an equal and free rational being with respect for all differences arising from gender, beliefs, status and overall attitude towards life including death (Observe, Orient, Decide, and Act) (Marra, Mcneil, 2012: 10). The robot must make a decision that is limited most by the existing built-in technology. Autonomy

versus automation is measured by the frequency of external operator interactions or independence from it, a measure of how the machine cope with the uncertainty of the environment, and the degree of reliability of decisions that the machine can make on its own (Marra, Mcneil, 2012: 18-19).

2.2. Development of drones and basic issues in their application and legal regulation

It is indisputable that technological capabilities have given capacity to drones for different purposes, but the different sizes of their platforms give them different opportunities to stay in the air. Their purpose ranges from combat missions to various forms of reconnaissance, transport, search, scientific exploration and rescue (Office of the Privacy Commissioner of Canada, 2014:5). It is the convenience of drones to be equipped with different and numerous sensors that enables them to track changes from a distance through the visible spectrum, electromagnetic spectrum, biological and chemical changes, with the ability to automatically detect target objects, to track positions through GPS systems, to register changes in real-time high-resolution cameras, giving huge potential for police use. This refers primarily to monitoring the condition of objects and their security, the movement of masses and individuals, to the point that they can be armed with different weapon systems (Schlag, 2013: 8). Drones, thanks to their unique sensors, represent a good platform that can be used even in operations, especially where it is dangerous or impossible to reach for humans or in times of extreme weather. The expansion of the potential and use of drones is a challenge for legislators, first and foremost, to protect the privacy interests of citizens, but also to regulate the use of these platforms by the police for their purposes. Almost identical situations of the use of surveillance devices are treated differently. In situations involving the use of human-powered airplanes and helicopters where extreme technological reconnaissance facilities are deployed, they are permitted without a court order, and at the same time, the use of drones is restricted to some routine police activities such as environmental monitoring and surveillance (McNeal, 2014: 2). Basically, countries that have regulated the use of drones prohibit the use of surveillance devices from drone platforms, while allowing the use of these assets in situations where they are not on the platform of the drones, e.g. cameras on the streets (McNeal, 2014: 2). Fear is a major driver for these kinds of solutions, because it suspects that the use of drones, that are much cheaper than human-operated aircraft, will result in widespread use of surveillance. Those opposed to these solutions state that in most cases these aircraft can carry less intrusive equipment than large

aircraft. Smaller aircraft, on the other hand, are cheaper than helicopters and human-powered aircraft, but unmanned aerial vehicles used by the military have powerful sensors are much more expensive than these classic human-operated aircraft, requiring not only the high cost of aircraft but also the fixed costs of many crews on land. Supervision of individuals and groups within society takes place on two tracks and with two patterns specified and diffused. Specific surveillance is performed on individuals who may be aware that they are in control or completely unaware of this fact, while diffuse control is exercised over a wider area or a wider range of subjects and more attributes that are collected to detect possible differences between normal patterns of behavior and those who can be described as deviants, in the case of traffic and crime control. Mostly the debate is over whether drones should be used for pro-active or post-event surveillance. There is agreement that they should not be used to proactively monitor and collect information about individuals and groups, and that they should not be armed (Office of the Privacy Commissioner of Canada, 2014: 45-46). The acceptability of drones as an intelligence tool is that they can integrate a great deal of data and behavior patterns of the individuals they follow. The data collected by the algorithms are linked by integrating data of private and public character. The question arises not only of public use but also of private use. The extent to which drones, by their presence, register only the outward-visible phenomena in one's life, as if one from a high hill observed behavior in public space, and to what extent they entered into the essence of one's life, intimacy and privacy, remains unanswered and unknown. In any case, whether looking at a specified individual as an object, or viewing an individual as a randomly selected object within a group to create a picture of a situation at a particular place at a particular time, there must be legal justification for both targeted and diffuse surveillance. Otherwise, it leads to an impact on the individual's right to assembly, the right to speak, and other freedoms in society, because it leads to an excessive intrusion of power into the individual's privacy. Private entities also have an interest in using and developing their own unmanned aerial platforms, which gave impetus to this industry which in 2012 force the US Congress to enact an act seeking to integrate the use of drones in airspace and their air control. This limits internal security to the use of drones for situations where police surveillance can be reasonably expected, such as at public meetings and events. However, similar surveillance of public space by a police officer from a tall building or helicopter is not prohibited, nor is surveillance of those same streets with fixed cameras. In addition to this technology-focused approach, there are proposals to create another approach that has ownership of the property or space in focus. Intention is to limit the duration of surveillance or time during which the drone may be in a particular space, to create measures of openness in

terms of insights in recorded materials, liability measures for those who use the drone, to protect privacy much more than in situations where human-powered aircraft use same technology (McNeal, 2014: 4). Comparisons are often made in relation to a closed system of television surveillance over a public space that is in the function of creating "situational awareness" and surveillance, but in practice they are a source of operational awareness of the behavior of people that are collected, stored and reused, although the attitude is that these cameras are for the purposes of public safety, not privacy collection. This was accepted by the public and there was no significant opposition to it. It is to be expected that when drones reach a certain critical point in both public and private use, the necessary "reasonable level of privacy expectation" with respect to the use of drones will be defined. However, unlike cameras set up in the streets or in a private area where citizens are aware that they are under surveillance, in most situation of drones' use where this is not the case, they will be conscious only post-facto, which is a completely different situation when it comes to adjusting their own behavior and legal consequences. The main difference between drones and closed camera surveillance systems is that drones can go anywhere, can change locations as well as real-time technology for recording and positioning. That makes much more difference from a legal and real point of view at drones than from a public space view line of optical visibility (Engelberg Center on Innovation Law and Policy, 2015: 7). Drones provide another advantage in multiple-positions and multiple-drones visual monitoring processes and the ability to integrate this technology with other technologies and exchange information in accordance with data management practices. The basic question in regulating the use of drones is the question of how far drones can go in collecting individual data in relation to the function of generating general awareness of the state of what is being observed. The question is also whether the drones move the quality of individual data collection over other systems and platforms, how it is managed, and whether that data complies with the law governing the protection of personal data (Office of the Privacy Commissioner of Canada, 2014: 6).

3. The legal question of usable drones

The right to privacy, or protection against unauthorized search of a person, apartment, correspondence and seizure of these items, is under the guarantee of the Fourth Amendment according to the United States Constitution. The US federal government has a history of regulating surveillance by police agencies through statutes / laws regulating wiretapping and recording that will be updated

with drone use regulations. This statute will guarantee the minimum privacy protection and will define, at the federal level, the level of protection that individual states will have for police use of drones. These statutes will be much less relevant for the private use of drones for the same purposes. It is likely that the private use, which involves video recording, photographing with the drones (which are much more complex for legal regulation), will be left to the federal states (Kaminski, 2013: 59). When it comes to the private use of drones in America, the most relevant regulation is the First Amendment of the US Constitution. The federal government and some countries agree that a court order is required for police use of drones, while private use involving traditional activities such as face recognition via drones, tracking the location and location of certain persons, and video recording is much more complex and harder to regulate (Kaminski, 2013: 60). Although the Fourth Amendment of the US Constitution has been sufficient to protect privacy so far from unauthorized intrusion, the development of technology has called into question its substance, since it was not intended for any technology that is present now or it would be present in the future. The Supreme Court has considered the issue of privacy through several cases (Schlag, 2013: 12-15), of which the significant case is Katz v. United States of 1967, which defined the perimeter within which an unjustified search could occur. In this case, it was an eavesdropping on a public payphone used by a person who reasonably expected the payphone to give her privacy in communication because the subject of control was person, not property, which in this case was public. In this case, the police violated the privacy provisions. The second case concerned aerial surveillance and concerns was the case of California v. Ciarolo in which police used aerial surveillance without an express court order and the object of the observation was the courtyard of the house, which was not visible from the outside and cannot be said to be accessible to the public. However, in this case, the court ruled that the landlord cannot reasonably expect that there was a right of privacy for aerial observers who could clearly see that he was growing marijuana in his yard and therefore had no right to protects himself using the Fourth Amendment. In the case of Dow Chemical v. The United States, Supreme Court has assessed that police had the right to conduct an aerial inspection in accordance with the Air Cleanliness Act, and that the filming of a chemical plant complex is not a search and interference with privacy under the Fourth Amendment. Search involves a physical search of space, and an insight into what is already visible as an open area is not a search. The very act of reconnaissance was carried out from public air traffic, which does not seem to be illegal. In the case of Kyllo v. The United States court found that using sensitive intrusion technology inside one's home to gather information is subject to the Fourth Amendment and it was treated as a

search. These actions also include the use of thermal cameras to read what is happening inside one's home. The use of the Katz test can also be applied to the use of radar to scan someone's home. This equipment is not intended for general use in public places, and therefore citizens are not expected to take measures to protect themselves from such intrusion into privacy. In the case of United States v. The Jones, Supreme Court concluded that the placement of Global Positioning and Vehicle Tracking Equipment was a search protected by the Fourth Amendment, with the addition that in this case the court invoked not only the right to expect privacy but also the very importance of property ownership. In this case, the installation of such a device is also a wrongful entry into possession. In the case of California v. Ciraolo (McNeal, 2014: 7) police reported that someone was growing marijuana in the yard of Mr. Ciraolo's house. Because the courtyard is enclosed by a fence and there is no way of seeing the inside of the garden, the police hired a private jet to make a 1,000-foot observation with the naked eye, which, according to FAA regulations, is a public flying area. The court held that the landlord could not expect privacy protection from public view and gave an example on which the decision was based. E.g. that climbing a two-story bus and looking over the fence would not violate privacy, and thus, even from public airspace for the purpose of navigation, privacy could not be violated. In the case of Dow Chemical Co. The Supreme Court analyzed the use of air reconnaissance helicopters, and in the case of Florida v. The Riley Supreme Court ruled that police did not need a court order to conduct aerial reconnaissance and naked-eye surveillance from public air traffic from a height of more than 400 feet to see what was already visible to the naked eye. The conclusion is supported by the fact that flying at that altitude it leaves no sound, no dust, wind, threat or injury to the property below, and that no detail of privacy regarding the use of that property was observed. The opinion of one of the court rulers was that a helicopter flight below 400 feet altitude, although safe under the regulations of the air navigation agency, would violate the expected privacy of those on the land being flown. By these judgments, the court allowed police to observe private and public property from the air under the aforementioned conditions in the same way that a passenger of any commercial aircraft can observe objects on the ground. In the United States, the Supreme Court based its reconnaissance position at an altitude from which the earth's position could be viewed with the naked eye. He went on the logic that when one sees what is clearly visible from the public space does not constitute a violation of the right to privacy and the Fourth Amendment. However, for police use, drones would technically have to fly below 500 feet and thus would obviously violate the adopted privacy principle and the principle of flying in public airspace. In the case of United States v. The 1946 Causby, Supreme

Court considered the case of a farmer whose land was located near a local small airport used by the military and whose planes were flying at low altitude of 80 feet over a farm. Those flights caused the death of the hen he kept on the farm. The court has applied a common law doctrine that says that if someone has the land he is also entitled to the heaven (air) above that land. Although in modern conditions this principle cannot be absolutely applied, the court has nevertheless found that the height above the land over which the landowner is entitled depends on the type of activity carried out on it and the landowner must be enabled to carry them out without adverse consequences. This created the doctrine of two types of airspace. One concerns public airspace in which air traffic is permitted and one below a certain height at which the owner has the right to exclude the use of aircraft (McNeal, 2014: 7-8). Thus, the average height of a dwelling is 35 feet and in the Causby case the court ruled that the aircraft must fly above 83 feet, as damage to the farm owner was inflicted below that height. In the case of Riley, the limit was 400 feet in which aircraft models were permitted because above that altitude, the public air traffic space, defined by the FAA's air navigation agency, begins. A height of 1000 feet has been defined as permitted for surveillance in the Ciraolo case as well as by the FAA (McNeal, 2014: 9). The disparity of court rulings is a consequence of resolving the issue in a particular case. There is obvious unevenness, but enough to gain a single limit for the use of drones and surveillance from the airspace. Since the minimum is 500 feet high for the flight of aircraft, the drones used by the police from that height are unusable because of their size and technology. They are small aircrafts that can only operate effectively from 40 feet high (McNeal, 2014: 9-10). This height is a space that belongs to the landowner and he can exclude the aircraft from disturbing its possession. The question is whether the police have the right to use the drone at that height above the street, which is a public area and to look inside a private property close to street, much like a police officer who is observing someone's property located in the valley from a hill could observe property in a valley, and that question remains. The ambiguity of the legal solutions shows the very essence of the problem, as Judge O'Connor said in a dissenting opinion that if we assume that the police have a marvelous aircraft that does not create noise or any damage and disturbance on earth, it can see not only what individuals on earth do but also in much more detail, e.g. they read the book. Even though the standards regarding the altitude from which they are allowed to fly have not changed in accordance with the requirements of the FAA, then we can certainly ask whether the logic of plurality of court decisions then works to claim that human rights to privacy have not been violated (McNeal, 2014: 10). As can be seen from the above, government activities are quite regulated while cases where private use of drones does not

clearly protect someone's privacy can be found in court. The problem is that the scope of the First Amendment should be clearly specified. Countries such as Texas that released the Texas Privacy Act into procedures, H.B. 912 prohibit recording without the consent of the property owner, as well as the collection of images or other information by civilians. Banning civilians from using drones leads them to be denied legitimate and crucial information in whose collection they have an interest in and right, thereby denying the First Amendment and their right to speak. There is a conflict of two rights, one to privacy and the other to speak. Specifically, there is a tension here similar to the right to privacy and the First Amendment right to record police activities in a public area without their permission. In some countries, police arrest people who shoot without the permission of other citizens, but also uses the same law to arrest people who shoot police activities without their consent. So instead of protecting privacy, we have a limitation on insight into government activity (Kaminski, 2013: 61). The US courts have divided in ways how to treat these issues from the First Amendment angle. The First Circuit Court considers that this amendment gives a clear right to be recorded by the police. The Eleventh Circuit Court finds that recording in the public interest is subject to restrictions on the time, space, and modes of recording. The Seventh Circuit Court considered the crime of recording a conversation when all parties to the conversation did not consent to the recording, and held that the statute regulating this crime limited significantly more freedom of speech than is necessary under the First Amendment interpretation of these freedoms. The court considered and concluded that the police, recording in public, depends on the context and that they are public servants, so the recording depends on the public interest, but it is not said how broad the First Amendment right is (Kaminski, 2013: 62). Obviously, these two amendments depend on where the recording takes place and where the right to privacy correlates with the memory and experience of others. So private things happen in a public place, but public things also happen in a private place (Kaminski, 2013: 63). Countries that take ownership as a principle for protecting privacy, prohibit any recording and spying on private property without the owner's consent, but also limit the right of the press to cover political and other events, e.g. the amateur is not allowed to record visible pollution from a local factory that pollutes the air with its exhaust. Under pressure from interest groups, some countries have banned agricultural farms from being filmed. The First Amendment does not prevent a person from being arrested for unauthorized entry into someone else's property, but prevents a person from being arrested if they are legally located and recording material of public interest (Kaminski, 2013: 63). Countries have different standards in terms of privacy breaches as well as breaches of confidentiality. Complex states like the US have a federal

minimum level of protection at the first level, and states are allowed to strengthen and better protect privacy. Thus, at the federal level, the use of drones by the police is regulated by the Electronic Communications Privacy Act (ECPA), which provides the basis for requests and orders of the police surveillance court.

This covers person location tracking, video surveillance and biometric identification, or other emerging technologies. However, the private use of drones is more complex because the regulation is split between the federal level and the states (Kaminski, 2013: 65). There is not one single privacy law at the US federal level but sectoral regulations exist, e.g. one act regulates the sharing of health information; financial information, third party video recording etc. (Kaminski, 2013: 65). Privacy lawsuits can be divided into four types: public disclosure of private facts, intrusion into privacy whether physical or electronic, portraying a person in public in a light that does not correspond to reality, or false light, which is also a defamation, then the unauthorized use of someone else's name with the likelihood of some gain (Kaminski, 2013: 65). The emphasis is on the type of information, whether the information is as private as the way it was obtained. State laws apply to the private recording of tone and image and are subject to arrest and prosecution. Through the licensing process, the FAA should provide the most important role in privacy protection, which is transparency, so that those under surveillance are aware that they are subject to privacy breaches. Unlike street cameras, when citizens are aware that they are under surveillance, in the case of drones the role of the FAA is to prescribe who uses the drone to collect data by issuing a statement of where and when is going to record, how long it will collect data etc. The task of the government is to help those who request information on whether they have been subject to surveillance to obtain recordings and other information form the drone users. Each drone would carry radio identification similar to the plates on the car so that it could be identified. In this way, a drone that violates one's privacy could be identified by radio frequency identification ("RFID") "license plates" (Kaminski, 2013: 67). Many countries prohibit the wearing of masks that cover their faces in public for anonymity, but in the case of extensive use of drones, this practice would decriminalize and allow persons wishing to be anonymous to wear a mask on their faces (Kaminski, 2013: 67).

The states have laws that partially regulate particular areas, but they could also cover the issue of drones, and these are the following laws: state eavesdropping law, Peeping Tom laws, video voyeurism laws, paparazzi laws that regulate privacy breach through photography, video recording and sound recording (Kaminski, 2013: 68). Peeping Tom statutes criminalize observation through a keyhole or other hole, but in order to be punished the perpetrator must be caught in action. Video voyeurism statutes criminalize viewing, video recording and photographing

another person without their consent or knowledge and when done for sexual arousal. Some of the statutes require the entity to be disclosed in whole or in part, and some merely require that there was a reasonable expectation of privacy. Paparazzi statutes prohibit the use of special technology to invade celebrity privacy and personal celebrity space. The drone control laws provided with the certain procedures consolidate these laws and serve the courts to strike a balance between privacy and free speech (Kaminski, 2013: 68). And it follows that countries will not completely ban drone shooting, but will limit it in a socially acceptable way, that is, in certain situations. States may decide to ban certain forms of surveillance of certain locations, that is, the certain forms of surveillance can only be allowed at a certain time, then that the basis of defense in a press court will surely be the character of a public event or public figures, and that secret recording will be banned, etc. Some courts have found that even in a public place, individuals can reasonably expect privacy, e.g. if a person is in their underwear and is on the street, or in the case of a survivor of a car accident that took place in a public space (Kaminski, 2013: 70). The Federal Video Voyeurism Prevention Act of 2004 ("VVPA") indicates that persons have a legitimate right to expect the privacy of their shameful places, whether in a public or private place, and that they will not be subject or exposed to viewing. The Fourth Amendment, unlike the First Amendment, does not expect privacy in a public place, but legislators may also accept that persons in these places are also entitled to privacy. It can be clearly seen from the law as well as from judgments when surveillance is secret, when it is intrusive, or when it uses technology that is pervasive and impedes privacy, but does not say when it is random and when it is continuous. Drone surveillance laws will certainly cover and punish shootings that are targeted, not accidental, continuous, or involve specific entities and / or events that are realistically expected to have private nature. There are ideas that, instead of focusing on technology that is clearly not fixed in time and that represents citizens' fear, other criteria are the focus of legislation (McNeal, 2014: 4). Thus, the author whose work we have used recommends that the height at which the drones are located be used as criteria, which is the height on which public air traffic above private property is permitted and where the possibility of intrusion into privacy and damage to property on earth due to overflight is minimal. This has already been stated in court judgments. Another way to limit aerial surveillance is to limit the dwell time of the aircraft above a specific location or person, which should limit the total time for monitoring the facility and therefore the amount of information that can be collected. Then, the legislator must define the storage time for the recorded and collected material. All data should be deleted after a certain period of time, and those data that are to be preserved should be given adequate access, which would

in itself require suspicion and validity of the request. For the sake of transparency in the collection of data by drones and their flights, public services using drones should, on a periodic basis, publish all data on these flights in order to identify possible omissions and responsibilities. Also, geofencing should be included in drone technologies as a program, which should activate the alarm as soon as the drone exits a given path of motion, as well as auto-sequencing which automatically blacks out all material or portions of the image that are not relevant. The reason is ownership of the property and therefore an important focus of drone use, because this right is easy to determine, while flight altitude issues are subject to change and this is debatable. Because, as was said in the Causby case, a low-flying aircraft, but an untouchable one, also made an intrusion on it as a person who had been uninvited and illegally taken possession of it. The second question is whether the right to use drones from public lands can be exercised, but from that height as if viewed from a lofty public place on private property. If the answer is positive, it should also be possible and legally allowed to the property owner to exclude the public from accessing his property. Although helicopters can fly above 400 feet and as such can carry sophisticated surveillance equipment without a court order and sometimes lower, but never below 350 feet, the question is why there is a problem that drones from that height can fly without a warrant. The answer is that they are almost imperceptible at this altitude and also because they carry GPS devices and at any moment they can be accurately located. In the future balloons or airships that can stay in the air for a long time will be used and lawmakers should focus on harm from aerial surveillance rather than the type of platform being used (McNeal, 2014: 17). It is recommended that the legislator focuses on the timing of oversight so as not to allow the use of constant oversight. The authors we used as reference recommend that it is still better to define the exact time for all types of aircraft, since in this case the court has no problem finding violations. The third proposal is to adopt procedures for storing data and recordings as well as their access to that information. Later on, the basis of a high level of doubt e.g. there is a reasonable suspicion that the government might keep the footage of a person it has been monitoring for a long time and draw conclusions about the most intimate details of a person's life. The purpose of the procedures is to prevent or impede the subsequent use and access to this data. All data would be destroyed after a certain period of time and there would be no possibility of it being made public except in criminal proceedings, so that these materials would be treated as any CCTV camera footage on the street for these purposes. The data are kept up to 30 days, including the possibility of appeal during this period. After this period the data would be removed from the server accessible to the police and its access would only be possible under a court order and with a

level of reasonable suspicion. A further new proposal is that the legislator should establish accountability and transparency of data so that on a periodic basis, and should publish information on the platforms used for surveillance, whether or not they have a crew. The information should be published on the agency's website with a restriction on disclosure regarding ongoing criminal investigations (McNeal, 2014: 20). What scares citizens is that drones are invisible, autonomous and powerful platforms for various means of surveillance, and since they are not common in the everyday use of citizens, this then requires the protection of the Fourth Amendment. Many citizens in the United States and in other countries around the world are not familiar with the details of the application and capabilities of drones with regard to intrusion into privacy, so legal protection of that privacy must be made. That is the logic of the Supreme Court of America's judgments in the cases cited as well as the following principles and tests. As a basis for search and seizure or seizure of things, there is a test of reasonable treatment. The test of reasonable treatment of drones and new technologies for surveillance and invasion of privacy is very difficult to define. In reality, there is a gap between knowledge of a particular technology and its real capabilities and application. Individuals from general audiences who do not understand the application of technology do not expect its application to their lives and are unable to take privacy measures. In Katz's case, the main principle was a test of reasonable expectation of privacy, while in Kyllo's case it was the gap between the availability of technology information and the actual capacity to apply it in relation to privacy breaches (Schlag, 2013: 15). In relation to the use of drones by police and private entities, if citizens were aware of the capacity of drones and the fact that there are no measures they can take to protect themselves from high resolution cameras, from infrared cameras, from GPS tracking of movement, from other electronic actions to the individual, trust in privacy would be completely destroyed on a reasonable basis even inside their homes (Schlag, 2013: 16). The mere fact that drones used by police are much cheaper and more widespread than those used by the military seeks privacy protection through the Fourth Amendment. The basic point so far is that an order is only required from a court if the information being collected is required as evidence in criminal proceedings and for other purposes not. It is reasonably expected to limit the use of drones for longer monitoring purposes. The use of technical solutions that should be used is geofencing and auto redaction, which would be more effective in limiting invasion of privacy than using human crews (McNeal, 2014: 21-22). Geofencing implies that data is collected from specific locations, whereas the other information would automatically be blacked out or unavailable. By recording the soil at a particular location, the person's face present on that location would be covered and could only be discovered by court order

on valid reasonable grounds or probable suspicion. Integrating drones into everyday life involves integrating drones into a set of values such as privacy, trust, security, freedom of expression, community, etc. The design of these aircrafts must reflect precisely the attitude towards these values. Privacy protection, especially in light of potential opportunities of the UAS requests that the government take steps to ensure privacy, and agencies it that sense will, review existing policies and procedures regarding the collection, use, retention, and forwarding of information collected to protect civil rights and freedoms and will improve those procedures in accordance with privacy law to meet the following conditions: (i) collection and use will be for an approved purpose; (ii) the retention of information collected by the UAS that may contain identifiable information will not be retained for more than 180 days; (iii) the dissemination of information will not be made outside the agency that collected it unless the dissemination is required by law.

4. Conclusion

There is a big difference in how drone market themselves and what their actual use is. The advertising and sale of drones is based on two aspects, price and cost as well as the ability of drones to meet customer requirements based on the technological solutions offered in their background. In drone marketing, manufacturers represent their use in neutral terms as "imaging and monitoring, " leaving room for numerous applications. The civilian use of drones is controversial and there is ongoing debate whether to allow and for what purpose their use and under what legal restrictions. In some countries that have enacted laws and allowed drone use for police purposes, a court order is required as a condition, and their use is treated as any other significant police or investigative activity. The paper, on the other hand, provides opportunities to limit the misuse of drones through legal solutions and with the use of technology that would itself be a brake on the misuse of drones, without limiting the number and purpose of drones only because of the fear of them. Solely because of the fear, society may impose a restriction on itself not to exploit the full potential of drones. This paper deals with the case law of the US Supreme Court as well as other courts related to the use of surveillance technologies that have been reported in the literature. This case law also becomes the benchmark for drones. In addition to reviewing the Fourth Amendment from the US Constitution, the use of drones under the First Amendment in the same constitution is also highlighted, in light of the use of drones for the purpose of journalism, hobbyists and other private initiatives that may lead to citizen surveillance not now by the government and its agencies but by other individuals or companies.

The existing legal regulations and case law are uneven and poorly adapted to the new technology, i.e. to the use of existing technology from new flying platforms such as drones. Various forms of their use make them far more dangerous to the privacy of citizens from whose use they have no real protection. This is why numerous factors need to be taken into account when it comes to limiting their use, as well as the factors that prevent hindering of privacy, if it is not based on a court order and a justifiable purpose.

References

- Engelberg Center on Innovation Law and Policy. (2015) *Drones & aerial robotics conference. Law & policy guidebook*. New York: Engelberg Center on Innovation Law and Policy.
- Kaminski, M.E. (2013) *Drone Federalism: Civilian Drones and the Things They Carry*. 4 Calif. L. Rev. Cir. 57, available at http://www.californialawreview.org/wp-content/uploads/2014/10/Drone-Federalism-CivilianDrones-and-the-Things-They-Carry.pdf,
- Marra, W. C., & McNeil, S. K. (2013). Understanding the loop: regulating the next generation of war machines. *Harv. JL & Pub. Pol'y*, 36, 1139.
- McNeal, G. (2014) *Drones and Aerial Surveillance: Considerations For Legislators*. Malibu: Pepperdine University School of Law
- White House, Office of the Press Secretary (February 15 2015) *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*. available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua
- Schlag, C. (2013). The new privacy battle: How the expanding use of drones continues to erode our concept of privacy and privacy rights. *Pittsburgh Journal of Technology Law & Policy, 13*(2).
- Stanley J., Crump, C (2011) Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft. New York: American Civil Liberties Union.
- Bracken-Roche, C., Lyon, D., Mansour, M.J., Molnar, A., Saulnier, A. & Thompson, S. (2014) *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada*. Kingston: Surveillance Studies Centre, Queen`s University.