DRONES AND THE ETHICAL POLITICS OF PUBLIC MONITORING

Andrei-Alexandru STOICA[*]

Ștefan PICA[**]

Abstract

This paper aims to analyze, from an ethical and legal point of view, the way in which drones are implemented and used for video monitoring. As such, we will focus on how drones have changed the legal landscape regarding public monitoring by state actors in situations regarding public safety, administrative and judicial tasks, but also during special events.

As such, the paper will evaluate the legal ramifications and instruments from EU and USA while comparing them to practices handled by the People's Republic of China. Furthermore, we will consider the ethical use of drones in conducting state activities. We will scrutinize the methods used by state agents in handling their tasks with drones, by comparing legal systems, using secondary data analysis and by having descriptive and correlational quantitative research.

The article also aims to identify if enough practice (administrative and legal) has been conducted to ensure that data protection has been safeguarded and whether interstate actions could pose a threat to the rule of law. In essence, we will interpret important case law from USA and Europe regarding the usage of cameras and other video monitoring devices, stationary and mobile, and also to figure out if its applicable to drones. If said legislation or legal practice exists and if not, we will spell out if its ethical or not.

Keywords: *drones, ethics, international law, public monitoring, European law.*

1. Introduction

Drones or unmanned aerial systems are a common sight in some states, but due to legal constraints have not been able to fly unrestricted. These restrictions have been in place to safeguard public health and property and will remain in place for a period of time until technology ensures an automatic response most issues.

The need for drones as mobile surveillance devices has been noted in the USA as early as the year 2013[1] when local legislatures adopted specific norms in order to allow law enforcement agencies access to drones for long range monitoring of public events, traffic or to enforce court mandates.

Other authors have noted that drone surveillance will ensure efficient means towards protecting remote and fragile environments. Unmanned Aerial Vehicles (UAV) allowed researchers and analysts to collect data in Antarctica and other special protected zones (Canada, New Zealand and others) without having to venture in hard to reach zones while gathering important data regarding climate changes[2].

Urban monitoring is important for state authorities and drones offer an elegant and cost-efficient solution for gathering information on traffic volume, observing accidents and finding potential law violations, yet the technology has yet to efficiently identify all participants and their goods[3].

Some authors consider that smart traffic monitoring is a key component in lowering car accidents and that a multi-UAV-network could decrease accidents by using drones to monitor the flow of traffic as to check for violations or to analyze a possibile accident based on the network data. The authors identified that Saudi Arabia

[*] PhD Candidate, Faculty of Law, „Nicolae Titulescu" University of Bucharest; Legal counselor for the Romanian Customs Authority (e-mail: andrei.stoica@univnt.ro).

[**] PhD Candidate, Doctoral School, Polytechnic University of Bucharest; IT engineer at the Romanian Customs Authority (e-mail: stefan.pica@cyberservices.com).

[1] G. McNeal, *Drones and aerial surveillance: Considerantions for legislatures*, Brookings Institute Report, November 2014.

[2] B. Bollard, A. Doshi *et al.*, *Drone technology for monitoring protected areas in remote and fragile environments*, Drones, vol. 6, no. 2, pp. 1-11.

[3] E.V. Butilă, R.G. Boboc, *Urban Traffic Monitoring and Analysis Using Unmanned Aerial Vehicles (UAVs): A Systematic Literature Review*, Remote Sens, 2022, vol. 14, 620, pp. 1-28.

has started using drones for traffic management and preliminary checks showcased that unmanned vehicles lowered by a small percentage the number of law violations[4].

We consider that such by using a UAV-network to monitor potential violations could decrease the number of incidents that happen in the European Union, seeing as how the European Commission released a study, in 2023[5], that highlighted a growing number of accidents in the EU, where Romania has been noted as the deadliest of the Member States.

However, ethics regarding the usage of unmanned aerial vehicles have led some authors[6] to study the usage of drones over groups of people and noticed that gathering information could be a privacy violation since it lacks a proper mean to obtain consent from the person or groups of persons that it flies over. Furthermore, it was considered that the psychological well-being of people could be affected since some groups did not know if the drones were used for their well-being or to illicitly spy on them so they engaged in conspiracy theories.

As such, we will focus on how drones can be used ethically in situations seeing as how starting with the year 2023 these vehicles have started being included in state and economical activities. Up to this point in history, drones had a certain usage in military operations as efficient intelligence gathering tools[7] and ever since the Nagorno-Karabah and Ukrainian-Russian conflicts, these vehicles started being used during armed conflicts as main means and methods of warfare.

2. Analysis of the way of implementation from a legal point of view

The United States of America have been a major state in how the usage of drones have been handled by state authorities seeing as how 27% of their police agencies[8] acquired at least one surveillance drone and 70% of the public authorities that have used drones were law enforcement agencies. Missions conducted by the law enforcement agencies had objectives such as search and rescue, crow monitoring and surveillance, traffic collision reconstruction, crime scene analysis and reconstruction, investigation of active shooters incidents.

The European Union has yet to adopt drones in such great numbers as most acquisition projects regarding drone implementation are scheduled to be conducted by the end of the year 2027[9] and some states, such as France, have had legal issues with how data protection has been handled with the usage of drones. As such, we mention that the Council of State has ruled that the Paris Police Prefecture is not allowed to use drones to monitor public demonstrations, both traditionally and with artificial intelligence blurring[10].

However, other states such as Italy, Greece and Spain have been using drones to monitor borders and the flow of migrants that are in transit to the EU and to try and either help those in need or to coordinate with other states to take them back[11]. Some[12] argued that the usage of drones similar situations could be seen as disproportionate and unethical since authorities deny access to asylum rights while other cases noted that the information sent from an EU state to a tertiary state allowed persons to be captured by other interested parties and sold into slavery.

These types of actions may violate some core principles in how drones can be used seeing as how in the Riga Declaration on remotely piloted aircraft[13] it was considered that: *„Drones also pose potential security risks. The design of drones can and should take into account those risks by using methods such as cyber-defence or geofencing. However, the malicious use of drones cannot be entirely prevented by design or operational restrictions. It is the task of the national police and justice systems to address those risks."*

Despite the Declaration not being legally-binding, the core principle of preventing abuses is the attribute of state authorities, meaning they have to also conduct proper investigations to how these operations have been

---

[4] N.A. Khan, N.Z. Jhanjhi *et al.*, *Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs)*, Computer Communications, vol. 157, May 2020, pp. 434-443.

[5] According to the European Commission study that can be accessed at *https://ec.europa.eu/commission/presscorner/detail/ro/ip_23_953*, accessed at 23.03.2023.

[6] A. Kannan, P. Ranganathan, Sminu T.V., *The Ethics of Utilising Drones in Wildlife Conservation and Monitoring*, Conservation India, 27.07.2020. C. Sandbook, *The social implications of using drones for biodiversity conservation*, Ambio, vol. 44, 2015, pp. 636-647.

[7] A. Hopkins, *The Ethical Debate on Drones*, Augustana Digital Commons, 2017, pp. 1-17.

[8] C.J. Smith, *How police departments are using drones*, Adorama, 17.06.2022.

[9] Statewatch, *„Next generation" armed drone with police potential tipped for EU financial backing*, Statewatch, 04.10.2021.

[10] *Idem*, *France: Court bans drone surveillance of demonstrations*, Statewatch, 13.01.2021.

[11] P. Burt, Jo Frew, *Crossing a line - The use of drones to control borders*, Drone Wars UK, December 2020, pp. 13-15.

[12] *Idem*, p. 19.

[13] Riga Declaration on remotely piloted aircraft (Drones) - *Framing The Future Of Aviation*, 06.03.2015 as published on the website *https://eu2015.lv/images/news/2016_03_06_RPAS_Riga_Declaration.pdf*, accessed at 24.03.2023.

conducted and how the data transmitted from the EU to non-EU states has been sent. We consider this a very concerning aspect seeing as how the European Court of Justice has stated in the *Schrems* case[14] that in the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.

Regarding the level of protection required in respect of such a transfer, the Court holds that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter.

In those circumstances, the Court specifies that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.

The European Court of Justice outlines that data protection towards third parties has to comply to the GDPR regulation and as such any information must be only transferred to states that ensure protection of this data. However, the lack of proper oversight of how data transfers are being handled and how drones gather said data could be considered a misuse and must be cross-examined as such[15].

It's important to note that the EU must identify the proper means to conduct drone operations seeing as how the European Commission considers unmanned aerial vehicles an important part of the future smart and sustainable ecosystem of European transport of goods and services[16]. The Drone Strategy 2.0 envisions network security for drones as to combat malicious use and to protect unmanned aerial vehicles from hacks.

However, there are more steps needed as to ensure that the strategy can be implemented since it only outlines proper means for authorities to tackle drone misuse, as such we recall that any drone handler has to abide by the CJEU decision in the *Rynes* case[17] which states that video surveillance by individuals that is carried out, even partially, in a public space is subject to the EU's Data Protection Directive, even if the camera capturing images of people is directed outwards from the private setting of the person processing the data.

The EU has been keen on regulating the usage of how drones gather information and as such has integrated unmanned aerial vehicles in its strategy regarding artificial intelligence in Europe as part of a system that display intelligent behaviour by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals[18].

The European Commission further emphasizes that human oversight of how data is being collected and handled will be a core principle for any technology that has a data stream that requires a built-in network[19]. As such, the autonomous behaviour of certain AI systems during its life cycle may entail important product changes having an impact on safety, which may require a new risk assessment. In addition, human oversight from the product design and throughout the life-cycle of the AI products and systems may be needed as a safeguard.

Union product safety legislation could provide for specific requirements addressing the risks to safety of faulty data at the design stage as well as mechanisms to ensure that quality of data is maintained throughout the use of the AI products and systems. The opacity of systems based on algorithms could be addressed through transparency requirements.

Furthermore, the European Commission has noted in its safety and liability implications of artificial intelligence report[20] that the operation of some autonomous AI devices and services could have a specific risk

---

[14] CJEU Judgment in Case C-311/18, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*.

[15] S. Fox, *Policing: Monitoring, investigating and prosecuting 'Drones'*, Brill Academic Publishers, 01.03.2019, pp. 1-33.

[16] European Commission, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions - A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', Brussels, 29.11.2022 COM(2022) 652 final.

[17] CJEU Judgment of the Court in case C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014.

[18] European Commission, Communication from the Commission, Artificial Intelligence for Europe, Brussels, 25.04.2018, COM(2018) 237 final, p. 1.

[19] European Commission, White paper on artificial intelligence - a European approach to excellence and trust Brussels, 19.02.2020 COM(2020) 65 final, pp. 20-22.

[20] European Commission, The opacity of systems based on algorithms could be addressed through transparency requirements, Brussels, 19.02.2020 COM(2020) 64 final.

profile in terms of liability, because they may cause significant harm to important legal interests like life, health and property, and expose the public at large to risks. This could mainly concern AI devices that move in public spaces (*e.g.*, fully autonomous vehicles, drones and package delivery robots) or AI-based services with similar risks (*e.g.*, traffic management services guiding or controlling vehicles or management of power distribution).

The challenges of autonomy and opacity to national tort laws could be addressed following a risk-based approach. Strict liability schemes could ensure that whenever that risk materializes, the victim is compensated regardless of fault. The impact of choosing who should be strictly liable for such operations on the development and uptake of AI would need to be carefully assessed and a risk-based approach be considered. Despite these warnings, the EU has yet to adopt a regulation on artificial intelligence seeing as how the proposal is still being worked on[21] and its currently entitled Artificial Intelligence Act.

The proposal for regulation does not identify drones or unmanned vehicles in a direct approach, however it covers all devices and vehicles that have autonomous or artificial intelligence capabilities, while also regulating biometric data and how high-risk systems can be sold by specialized vendors.

Drones are regulated in the European Union and European Economic Area with the help of the European Union Aviation Agency which has helped lawmakers adopt a common core of regulatory norms for how unmanned vehicles are allowed to fly[22]. These regulations have strict data security provisions and as such both users, manufactures and importers have to abide by the ethical standards on how cameras and other data gathering tools are being used and force the users to learn and understand basic concepts of data and privacy protection.

Furthermore, automated processing of information has to be handled by the General Data Protection Regulation[23] for all devices that are developed in the EU or imported from third party states. This translates to an obligation to all users to fully understand what types of information their device gathers and what should be done with the p

In other states, such as the United States of America or the People's Republic of China, public monitoring has been conducted in various ways, depending on the legal instruments applicable to said geographical area.

In the United States of America only a small number of states have adopted specific regulations regarding how drones can capture, store and use information gathered with its optics or other means of data gathering tools[24]. Most of the states from USA prohibit the gathering of data from other persons without their consent, while other states also limit public authorities in obtaining data with the use of drones without a mandate.

Data gathered with the usage of various drones showcases different types of information and metrics meaning that some unmanned vehicles gather a data of a higher quality than others and can even analyze the information in real time or can predict certain actions of a person or group[25]. The metrics obtained show that it is possible to efficiently integrate state-of-the-art artificial intelligence models in a drone as new functionalities, embedded in the command and control device used to pilot the drone. In situations such as the COVID-19 pandemic, where strict control of capacity was needed, or other more common situations where large areas need to be kept within capacity limits, we have shown the possibility to easily add existing and improved deep learning detection models in the command and control of the drone for helping law enforcement agents.

---

[21] For reference, the proposal can be accessed at *https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence*.

[22] For reference, Regulation (EU) 2018/1139 of the European Parliament and of the Council of 04.07.2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) no. 2111/2005, (EC) no. 1008/2008, (EU) no. 996/2010, (EU) no. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) no. 552/2004 and (EC) no. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) no. 3922/91 (text with EEA relevance), published in OJ L 212, 22.08.2018; Commission Implementing Regulation (EU) 2019/947 of 24.05.2019 on the rules and procedures for the operation of unmanned aircraft (text with EEA relevance), published in OJ L 152, 11.06.2019 and Commission Delegated Regulation (EU) 2019/945 of 12.03.2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems published in OJ L 152, 11.06.2019.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 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) (text with EEA relevance), published in OJ L 119, 04.05.2016.

[24] As seen on the website *https://www.findlaw.com/consumer/consumer-transactions/drone-laws-by-state.html*, accessed at 28.03.2023.

[25] P. Royo, A. Asenjo, J. Trujillo *et al.*, *Enhancing Drones for Law Enforcement and Capacity Monitoring at Open Large Events*, Drones, vol. 6, no. 11, pp. 1-22.

In the case of the People's Republic of China, most regulations regarding the usage of drones are similar to those of the European Union or the United States of America[26], meaning we are in a standardized environment on how and where unmanned vehicles can operate, the data gathered while operated (flight data, telemetries and others) are uploaded directly in the civil aviation authority database.

Such situations have sparked a debate on whether or not lawmakers should ban Chinese drone technology because of the information and lack of proper control mechanisms on where and how it is stored. While the EU has yet to tackle the subject in a broad sense, some states, such as Lithuania[27], have started restricting drone imports from certain states that do not uphold a proper data security code of conduct.

These types of legislative measures have been firstly registered in the USA where a Countering CCP Drone Act was proposed in Congress[28] and it focuses on restricting certain types of drones and manufacturers from distributing said goods in shops.

These measures were adopted since a lot of data obtained with goods built in certain states who are known to disregard basic data protection rights seeing as how a lot of data was gathered during a crisis and said data was then sent overseas.

We consider that the EU should either adopt better means in protecting its citizens from unwanted spying as the issues that arose from the Pegasus spyware scandal have not been fully handled by states and the Commission. The European Parliament, in its study of the phenomenon, found that «*On 19 April 2022, the EU Commission stated that it will not investigate Member States that used Pegasus to spy on politicians, journalists and other individuals, as „this is really something for the national authorities", and that the EU commission cannot deal with national security issues: people should seek justice at national courts' level*»[29].

The Pegasus spyware was used illicitly, as the European Data Protection Supervisor outlined[30], that a ban on the development and deployment of intrusive software should be adopted by the EU and as such, we consider a similar approach should be implemented to drones which do not offer a protection of intrusiveness.

3. Study on the ethical use of drones

The ethical usage of drones relies on how efficient artificial intelligence and other automated data processing software and devices interact. As such, we would like to point out a few situations that could be applicable to drones.

One such situation is the capacity of a video mounted on an unmanned aerial vehicle to falsely identify a target and to release a wrongful statement regarding the target's activity. For example, in China, a picture of the chairwoman of Gree Electric Appliances had her face displayed on a huge screen erected along a street in the port city of Ningbo that displays images of people caught jaywalking by surveillance cameras. The artificial software used by the traffic police erred in capturing Dong's image from an advertisement on the side of a moving bus[31]. This led to the police issuing a wrongful accusation and fined the person for unlawful conduct. It was later cleared up.

A similar issue was noted in the United Kingdom where women with darker skin are more than twice as likely to be told their photos fail UK passport rules when they submit them online when compared to lighter-skinned men, according to an investigation. A black student, said she was wrongly told her mouth looked open each time she uploaded five different photos to the government website. This shows how *„systemic racism"* can spread. The facial recognition software was used by the Home Office of the British government to help users get their passports more quickly. Additionally, another person, who describes her complexion as dark-skinned, told

[26] J. Ma Eiger, *Drone regulations in China,* Lexology, 19.01.2021; L. Hao, *Regulations of UAS in China*, ICAO, 2020, presentation accesed at *https://www.icao.int/Meetings/Remotetech/Presentations/Day2_Session%206_%20RPAS%20Stream_Liu%20Hao.pdf* at 28.03.2023.

[27] B. Crumley, *Lithuania's new public IT procurement ban covers drones from China, Russian, and Belarus equipment,* DroneDj, 05.12.2022.

[28] Legislative proposal H.R. 6572, the text can be read at *https://www.congress.gov/bill/117th-congress/house-bill/6572?s=1&r=2*, accessed at 28.03.2023. G. Corn, *The legal aspects of banning Chinese drone technology*, Lawfare, 04.02.2021.

[29] O. Marzocchi, M. Mazzini, *Pegasus and surveillance spyware*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 732.268 - May 2022, p. 15.

[30] *Idem*, p. 17.

[31] According to the AI incident database website, editor Sean McGregor, accessed at 28.03.2023 at *https://incidentdatabase.ai/cite/36/#r595*.

investigators that her photos have been judged to be poor quality which included *„there are reflections on your face"* and *„your image and the background are difficult to tell apart."*[32]

Furthermore, Human Rights Watch points toward a possibility where police could use unmanned devices in order to discriminate targets based on certain data that was uploaded to the devices database[33]. This was mostly recorded in China where the police use drones to identify the Muslim minority and use specific operations against them.

An ethical and legal issue arose in the United Kingdom where a group of researchers from Cambridge University analyzed, in the year 2022, how some police departments used facial recognition technologies and concluded that violations on how data protection is handled, racial profiling and illicitly accessing mobile phones have been found[34].

This outcome is a far-cry seeing as how on august 11, 2020, the Court of Appeal of England and Wales overturned the High Court's dismissal of a challenge to South Wales Police's use of Automated Facial Recognition (AFR) technology, finding that its use was unlawful and violated human rights[35].

The Court found that South Wales Police's policies gave too much discretion to individual police officers to determine which individuals were placed on watchlists and where AFR Locate could be deployed. The Court commented that *„the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law."* The Court further described the discretion as *„impermissibly wide"*, for example because the deployment of the technology was not limited to areas in which it could be thought on reasonable grounds that individuals on a watchlist might be present. The Court implied that this should be a significant factor in determining where AFR Locate should be deployed, stating, *„it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watchlist are going to be at that location."*

We would also like to point out the North Dakota v. Brossart case[36] where the District Court of North Dakota allowed the usage of an evidence gathered by a Predator drone to capture and uphold an arrest of an US citizen after a stand-off with a SWAT unit, without the issuance of a warrant for drones.

These situations are just some of the events in which privacy was violated by the usage of drones and some of the only cases in which the perpetrator was able to be brought to justice, seeing as how the Federal Aviation Administration in the USA has thousands of reports[37] of unmanned vehicles that did not get a proper police investigation. Also, it is important to note that in the USA there are over 855.000 drones registered at the Federal Aviation Administration (as of 2023) and almost 92% of the waivers solicited by drone operators is for them to use their vehicles at night[38].

Other incident databases outline that drones have been used to violate privacy of persons while inside their home, disregard public safety limits and observe objectives in restricted airspace and to smuggle contraband[39]. While the number of incidents may be relatively small the implications and the problems are alarming since a lot of these cases are reported as public safety announcements. A lot more cases remain unchecked due to poor legal oversight or lack of resources to properly investigate breaches.

---

[32] According to the AI incident database website, editors Sean McGregor and Khoa Lam, accessed at 28.03.2023 at *https://incidentdatabase.ai/cite/87/#r1387*.

[33] M. Wang, *The robots are watching us*, HRW - Pen/Opp, 06.04.2020.

34 F. Lewsey, *UK police fail to meet 'legal and ethical standards' in use of facial recognition*, Cambridge University - Research, 27.10.2022.

[35] Royal Court of Justice, CA, Case no. C1/2019/2670, *R. v. The President of the Queen's Bench Division and others*, 11.08.2020. H.A. Kurth, *UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v. South Wales Police*, Huntonprivacyblog.com, 12.08.2020, accessible at *https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/*, accessed at 28.03.2023.

[36] District Court - Nelson County, North Dakota, *State of North Dakota v. Thomas Brossart and others*, Case no. 32-2011-CR, accessible at *https://www.nacdl.org/getattachment/136371f4-aa38-476f-bd9a-a0908dbfd19b/Brossart-Order.pdf?lang=en-US*, accessed at 28.03.2023.

[37] As seen on their website: *https://www.faa.gov/uas/resources/public_records/uas_sightings_report*, accessed at 29.03.2023.

[38] Statistics take from the website *https://skykam.co.uk/drone-statistics/*.

[39] As seen on the website *https://www.dedrone.com/resources/incidents-new/all*, accessed at 29.03.2023.

4. Conclusions

Drones can reduce risk to humans and offer new logistical connections. A study in the UK outlines that unmanned vehicles helped public authorities in over 500 incidents globally[40], yet the issue of data and network protection remains an unresolved issue that needs more funding[41].

The solutions to illicit public monitoring should focus on arming public safety agencies with the required tools to thwart threats to individuals and public agencies. However, we do not agree that the usage of military-grade drones, to counter or intimidate potential public events, should be allowed. Such a practice was seen in the year 2020 when a Predator drone flew over the city of Minneapolis to monitor the George Floyd protests instilling fear in regards to participating in public life and privacy[42].

As such, public authorities should arm themselves with both anti-drone weapons and specialized unmanned vehicles designed to identify and neutralize illicit vehicles that are being handled by unauthorized operators. This could help prevent situations in which drones were used to monitor special events (2014 - public speech of Angela Merkel or 2014 - Serbia – Albania football match) or important public objectives (2015 - White House drone crash)[43].

Furthermore, respect is a fundamental virtue in the sense that to respect a person is to value a person. Persons have the fundamental right of having their privacy respected. When drones are used to take photographs of a person or when a person is stalked by another person, their privacy has not been respected[44].

We consider that the only proper way to ensure that public authorities respect privacy and will enforce data gathering and management is by only acting based on an existing warrant. This should act both in means of public monitoring and in the case of anti-drone operations. The right to privacy includes data protection. As indicated, the police collect large amounts of information for the prevention, detection and investigation of crime. There must be safeguards in place to protect the collection, processing and sharing of data. The United Nations Inter-Regional Crime and Justice Research Institute propose that law enforcement agencies comply with the following requirements regarding data protection, namely fairness, accountability, transparency and explainability[45].

To respect citizen's fundamental rights and avoid potential liability, the use robotics in law enforcement should be characterized by fairness; accountability; transparency; and explainability. Some deployments of drones are similar to video capturing systems or incident response by police helicopter. Because they monitor public space, over-arching regulations are appropriate to these deployments, as long as the difficulties surrounding consent and access to data can be addressed. However, unmanned vehicles can be equipped with numerous other attachments (infrared cameras, microphones and others) and must have oversight or at least ensure traceability, because the equipment is both accessible to public agencies and private persons.

A legal solution would be that to consider drone usage as preemptively illicit as it requires technology to undertake visual surveillance, and as such will require proper oversight, both internally and externally as to ensure that the data captured through its optics will be deleted at some point or used only for its intended purpose. This approach has already been tested, as we have shown, since most Court decisions have shown that public authorities and people have not fully grasped the legal obligations that data protection implies.

We consider that a special task force that could use artificial intelligence and drones to counter potential physical assaults and data violations is the most accessible approach that any state can adopt. Such a specialized department was tested in Japan where an anti-drone task force conducted operations against potential hazardous drone incidents (such as the 2015 radioactive drone that was spotted on Japan's Prime Ministers house or the 2022 G7 Summit event where anti-drone technology was used to discourage illicit drone

[40] Rt Hon Kwasi Kwarteng (coord.) *et al.*, *Advancing airborne autonomy Commercial drones saving money and saving lives in the UK,* H.M. Government report, 18.07.2022, p. 16.

[41] *Idem*, pp. 44-46.

[42] C. Enemark, *Armed Drones and Ethical Policing: Risk, Perception, and the Tele-Present Officer*, Crim Justice Ethics, 2021; 40(2), p. 124-144.

[43] European Army Interoperability Centre, *Top 5 drone incidents*, FINABEL, 20.08.2019.

[44] R. L. Wilson, *Ethical Issues with use of Drone Aircraft*, IEEE, 2014, 978-1-4799-4992-2/14.

[45] A. Hazenberg, I. Beridze (coord.), *Artificial intelligence and robotics for law enforcement,* United Nations Interregional Crime and Justice Research Institute, 2019, pp. 12-13.

monitorisation of the event)[46] . This type of approach ensure that public authorities will properly defend both important state objectives and its citizens from technological threats without having to be a splintered force.

References

- G. McNeal, Drones and aerial surveillance: Considerantions for legislatures, Brookings Institute Report, Noiembrie 2014;
- B. Bollard, A. Doshi et al., Drone technology for monitoring protected areas in remote and fragile environments, Drones, vol. 6, no. 2;
- E.V. Butilă, R.G. Boboc, Urban Traffic Monitoring and Analysis Using Unmanned Aerial Vehicles (UAVs): A Systematic Literature Review, Remote Sens, 2022, vol. 14;
- N. Ali Khan, N.Z. Jhanjhi et al., Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs), Computer Communications, vol. 157, May 2020;
- A. Kannan, P. Ranganathan, Sminu T.V., The Ethics of Utilising Drones in Wildlife Conservation and Monitoring, Conservation India, 27.07.2020;
- C. Sandbook, The social implications of using drones for biodiversity conservation, Ambio, vol. 44, 2015;
- A. Hopkins, The Ethical Debate on Drones, Augustana Digital Commons, 2017;
- C.J. Smith, How police departments are using drones, Adorama, 17.06.2022;
- Statewatch, „Next generation" armed drone with police potential tipped for EU financial backing, Statewatch, 04.10.2021;
- Statewatch, France: Court bans drone surveillance of demonstrations, Statewatch, 13.01.2021;
- P. Burt, J. Frew, Crossing a line - The use of drones to control borders, Drone Wars UK, December 2020;
- Riga Declaration on remotely piloted aircraft (Drones), Framing the Future of Aviation, 06.03.2015,
- CJEU Judgment in Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems;
- S. Fox, Policing: Monitoring, investigating and prosecuting 'Drones', Brill Academic Publishers, 01.03.2019;
- European Commission, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions - A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', Brussels, 29.11.2022 COM(2022) 652 final;
- CJEU Judgment in case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11.12.2014;
- European Commission, Communication from the Commission, Artificial Intelligence for Europe, Brussels, 25.04.2018, COM(2018) 237 final;
- European Commission, White paper on artificial intelligence - a European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final;
- European Commission, The opacity of systems based on algorithms could be addressed through transparency requirements, Brussels, 19.2.2020 COM(2020) 64 final;
- Regulation (EU) 2018/1139 of the European Parliament and of the Council of 04.07.2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) no. 2111/2005, (EC) no. 1008/2008, (EU) no. 996/2010, (EU) no. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) no. 552/2004 and (EC) no. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) no. 3922/91 (text with EEA relevance), published in OJ L 212, 22.8.2018;
- Commission Implementing Regulation (EU) 2019/947 of 24.05.2019 on the rules and procedures for the operation of unmanned aircraft (text with EEA relevance), published in OJ L 152, 11.06.2019 and Commission Delegated Regulation (EU) 2019/945 of 12.03.2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems published in OJ L 152, 11.06.2019;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 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) (text with EEA relevance), published in OJ L 119, 04.05.2016;
- P. Royo, A. Asenjo, J. Trujillo et al., Enhancing Drones for Law Enforcement and Capacity Monitoring at Open Large Events, Drones, vol. 6, no. 11;
- J. Ma Eiger, Drone regulations in China, Lexology, 19.01.2021; L. Hao, Regulations of UAS in China, ICAO, 2020;
- B. Crumley, Lithuania's new public IT procurement ban covers drones from China, Russian, and Belarus equipment, DroneDj, 05.12.2022,
- Legislative proposal H.R. 6572 - US Congress;

[46] J. Vincent, *Tokyo police unveil net-wielding interceptor drone*, The Verge, 11.12.2015. H. Habuka, *Japan's approach to AI Regulation and its impact on the 2023 G7 Presidency*, Center for Strategic&International Studies, 14.02.2023.

- G. Corn, The legal aspects of banning Chinese drone technology, Lawfare, 04.02.2021;
- O. Marzocchi, M. Mazzini, Pegasus and surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 732.268 - May 2022;
- M. Wang, The robots are watching us, HRW - Pen/Opp, 06.04.2020;
- F. Lewsey, UK police fail to meet 'legal and ethical standards' in use of facial recognition, Cambridge University - Research, 27.10.2022;
- Royal Court of Justice, CA, Case no. C1/2019/2670, R. v. The President of the Queen's Bench Division and others, 11.08.2020;
- H.A. Kurth, UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v. South Wales Police, Huntonprivacyblog.com, 12.08.2020;
- District Court - Nelson County, North Dakota, State of North Dakota v. Thomas Brossart and others, Case no. 32-2011-CR; 33;
- R. Hon Kwasi Kwarteng (coord.) et al., Advancing airborne autonomy Commercial drones saving money and saving lives in the UK, H.M. Government report, 18.07.2022;
- C. Enemark, Armed Drones and Ethical Policing: Risk, Perception, and the Tele-Present Officer, Crim Justice Ethics, 2021; 40(2);
- European Army Interoperability Centre, Top 5 drone incidents, FINABEL, 20.08.2019;
- R.L. Wilson, Ethical Issues with use of Drone Aircraft, IEEE, 2014, 978-1-4799-4992-2/14;
- A. Hazenberg, I. Beridze (coord.), Artificial intelligence and robotics for law enforcement, United Nations Interregional Crime and Justice Research Institute, 2019;
- J. Vincent, Tokyo police unveil net-wielding interceptor drone, The Verge, 11.12.2015;
- H. Habuka, Japan's approach to AI Regulation and its impact on the 2023 G7 Presidency, Center for Strategic&International Studies, 14.02.2023.