

Balancing Security and Privacy - Challenges and Solutions for Regulating Police Drone Use

Łukasz Dziura¹

Abstract

Balancing security and privacy in the use of police drones is a complex challenge that requires critical steps in ensuring that police drone use aligns with democratic values and legal standards. By addressing these challenges and implementing thoughtful solutions, police agencies can harness the benefits of drone technology while safeguarding civil liberties and maintaining public trust. This article addresses two primary aspects. Firstly, it examines the challenges posed by the rapid adoption of new technologies by the police. Secondly, it presents findings from socio-legal research conducted between 2019 and 2023. This research combines doctrinal legal analysis with empirical studies carried out in Poland, Germany, Spain, and the United Kingdom. It incorporates in-depth interviews with police officers, officials, and international experts, alongside field observations. The article concludes with critical observations on current legislation, highlighting significant deficiencies, and advocates for a new approach to police accountability and transparency.

Keywords: Police; Drones; Privacy; Accountability; Policing

1. Introduction

The advent of drone technology has revolutionized various sectors, including law enforcement. Police agencies worldwide have adopted drones for tasks ranging from search and rescue operations to traffic monitoring and crowd control. While drones offer significant advantages in terms of efficiency and effectiveness, their use also raises profound concerns about privacy and civil liberties. Balancing the need for security with the protection of individual privacy presents complex challenges that require thoughtful regulation and oversight. This article explores these challenges and proposes solutions to ensure that police drone use aligns with democratic values and legal standards.

One of the primary concerns with police drone use is the potential invasion of privacy. Drones equipped with high-resolution cameras and other surveillance technologies can easily capture images and data from private properties adjacent to public spaces. This capability raises significant privacy issues, as individuals may be monitored without their consent or knowledge, leading to a perception of constant surveillance and an erosion of personal privacy. Such invasive surveillance can be particularly problematic in densely populated urban areas where private and public spaces often overlap. Drones differ significantly from CCTV cameras in their surveillance capabilities. While CCTV cameras are fixed in elevated positions to monitor specific areas, drones offer far greater flexibility. They are not stationary and can easily change positions, allowing them to cover much larger areas. More importantly, drones provide an aerial overview—the higher their altitude, the larger the area they can cover. This aerial perspective also makes it easier to look into private apartments, plots, and houses. Even if monitoring private spaces is not the primary intent of a police drone operator, it is almost inevitable that private property will be recorded while surveilling public spaces. Those privacy concerns have decreased public support for drone surveillance (Sakiyama et al., 2017). Research shows that, even when accounting for pro-privacy beliefs and anti-surveillance views, any type of drone surveillance activity—such as monitoring citizens around their homes, workplaces, or open public spaces—reduces support for police drones (p. 1029).

The rapid deployment of drone technology has often outpaced the development of comprehensive regulatory frameworks. Without clear guidelines and robust oversight mechanisms, there is a risk of drones being

¹Jagiellonian University in Kraków, Faculty of Law and Administration, Bracka 12, 31-005 Kraków, Poland
e-mail: lukasz.dziura@doctoral.uj.edu.pl

used arbitrarily or excessively. This can result in a lack of accountability for how, when, and why drones are deployed, leading to potential abuses of power. The absence of standardized regulations also creates inconsistencies in how different jurisdictions manage drone use, complicating efforts to ensure uniform protection of civil liberties. Those issues are not theoretical but have already led to city-wide ban of police use of drones in Paris. Paris officials argued that police drones violate freedom of expression, citing lack of proper oversight and regulations that would ensure accountability (BBC, 2020).

The vast amounts of data collected by drones necessitate stringent data management protocols. There are significant risks associated with data breaches, unauthorized access, and the misuse of collected information. Sensitive data could be exploited for purposes beyond law enforcement, such as personal vendettas or political surveillance, undermining public trust in police agencies. Ensuring data security and preventing misuse are critical to maintaining the legitimacy and effectiveness of police drone operations. Data collected by drones exacerbates the situation further. Drone operators can view live video feeds, and the data can be directly uploaded to the cloud. In the age of *big data*, drones intensify the challenges in surveillance and data collection, compounding concerns about privacy and security (Bennet-Moses, Chan, 2014, p. 651).

The opaque nature of drone operations can diminish public trust in law enforcement. Without transparency about drone usage policies, operational details, and accountability measures, the public may perceive the use of drones as intrusive and authoritarian. This lack of trust can hinder effective policing and community relations, as citizens may feel alienated and suspicious of law enforcement activities. A great example of this is the 2014 Ontario protests, during which a police drone hovering over the crowd provoked anger among the protesters. Despite the police's intention to use the drone for public safety, people perceived it as an escalation and a form of intimidation. The police later explained that drones provide a cost-effective method for photographing crowds. However, the protesters viewed the drone as military technology, which contributed to their negative reaction due to the drones' remote vision and piloting capabilities. One protester remarked, "*police bring military logic, technology, and experience squarely into the realm of policing and civil security*" (Bowman, 2014). This highlights the concept of how technology's perception is influenced by both aesthetics (perception) and politics (power dynamics) (Brighenti, 2007, p. 324). This concept underscores the significance of vision in surveillance. It not only involves seeing and being seen but also symbolizes the asymmetry of power and visibility. In the Ontario protest, this asymmetry led protesters to view the police not as a public security agency, but as an enemy exerting power over them. Direct eye contact fosters social relations, while the awareness of being watched without knowing by whom can be dehumanizing and increase feelings of aggression and distrust (p. 326).

Drones also face practical operational limitations. Their effectiveness is heavily dependent on weather conditions; high winds, rain, fog, and extreme temperatures can severely limit their capabilities. Additionally, connectivity issues in urban areas can lead to intermittent data transmission, compromising real-time monitoring and increasing the risk of operational failures. These technical challenges need to be addressed to ensure reliable and effective drone operations.

2. Methods

This article is based on legal research and empirical studies conducted in Poland, Germany, Spain, and the United Kingdom. These countries were chosen because, at the time the study was initiated, their national police forces (with the exception of Poland) were operating drones under extensive regulations. Throughout the study, the legal landscape in Europe underwent significant changes with the adoption and implementation of European Union regulations, which have influenced the use and regulation of drones across these countries.

There is a significant lack of research on the legal framework within the European Union concerning the implications of police drone use, particularly in areas such as privacy invasion, police accountability, and balancing the protection of citizens' rights with police effectiveness. Consequently, the initial part of this study concentrated on doctrinal legal research. This research method "*provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty, and, perhaps, predicts future developments*" (Pearce et al., 1987, p. 56). It involves a comprehensive analysis of legal provisions, rules, norms, guidelines, and the intentions, propositions, and principles of legislators. However, as Chynoweth (2008, pp. 28-29) points out, understanding legal doctrine alone is insufficient; it requires the application of legal rules and doctrines to specific facts. Furthermore, as Hutchinson and Duncan (2012, p. 85) note, although doctrinal legal research has long been a fundamental aspect of legal studies, there has been no recent need to explain or classify it within a broader cross-disciplinary research framework. They argue that the doctrinal method is often so implicit and unspoken that many in the legal field see no need to articulate the process. However, this method should be detailed and contextualized within the real world (p. 86).

Research was carried out on the regulation of police drone use in Poland, Germany, Spain, and the United Kingdom. This research covered both national and local legislation, internal police regulations, and court decisions where available. A general search using Google and Google Scholar was conducted to identify the most relevant issues and sources, leading to a more detailed examination of internal police regulations and court decisions. Some sources were more accessible than others. British legislation was the easiest to study, facilitated by the *Freedom of Information Act* and detailed information shared by Kent and Sussex Police on their websites. German regulations were also relatively straightforward to study, with ample available information and numerous academic papers on the topic. In contrast, researching regulations in Poland was challenging due to the lack of specific legislation and the reluctance of Polish police to share internal regulations with the public. The most difficult research was in Spain, not because of a lack of relevant regulations—Spain was chosen for its extensive legislation—but due to the scarcity of English translations. This language barrier also hindered empirical studies, as even the Spanish European Union Aviation Safety Agency (AESA) provided limited information in English on its website. To overcome these challenges, interpreters were employed on several occasions.

It is essential to note at this point that doctrinal legal research had to be conducted twice. Initially, this research was carried out during the early stages of the grant program. However, as previously mentioned, a new EU-wide legal framework was adopted and implemented into national legislations in December 2020. This necessitated repeating the doctrinal research, which proved extremely useful. Understanding the existing regulations in each country enabled a unique analysis of the implementation process from a national perspective. While Spain, Germany, and Poland had already aligned their legislations with the new regulations, the United Kingdom, having left the European Union, did not adopt the new system and is not a member of the European Union Aviation Safety Agency (EASA).

Building on the findings from the doctrinal legal research, empirical research was conducted next. This phase involved in-depth interviews with police officers, national aviation safety agency officials, and foreign experts in the field. Police departments and aviation safety agencies were contacted via email to request a designated individual willing to participate in an interview, while experts were approached directly to arrange meetings. Each email detailed the interview topics and the study's purpose. In some instances, requests for additional information about the interview structure and specific inquiries were made and addressed. Participants were informed that all interviews would be voice-recorded due to the nature of the study. Most interviews were conducted in person and on-site, while four had to be conducted remotely due to participants' scheduling conflicts, and one due to illness. Each in-depth interview was structured around a pre-prepared questionnaire.

In addition to the interviews, permission was granted on three occasions to observe police officers using drones in their work. The first observation took place in the UK, where the processes of preparation, flight, and after-mission reporting were demonstrated. The other two observations occurred in Poland, where police officers permitted observations during traffic control operations and provided insights into their usual procedures. Field notes were taken in all three cases to document the observations.

3. Results

The following section presents the results from doctrinal legal research, in-depth interview responses, and field study observations. The first subpart outlines the current state of legislation in the United Kingdom, the EU, Spain, Germany, and Poland. The second subpart covers: a) the most common use cases for police drones, b) officer attitudes towards drones and the implications of their use on privacy, and c) notes from limited field observations on the practical use of police drones.

3.1. Legislation

In the European Union, two key legislative acts regulate the use of drones by the police. The first is *Regulation (EU) 2018/1139*², which aims to create a unified airspace within the EU and requires police officers to follow the same certification, testing, and operational rules as civilians when flying drones, with minor exceptions. While specific regulations, airspace classifications, and types of drone missions are beyond this study's scope, one notable provision mandates that individuals not involved in a drone mission be informed when such a mission is ongoing, necessitating drones to have bright lights for increased visibility.

²Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency (EASA).

The second significant act is *Directive (EU) 2016/680*³, which mandates that all member states protect citizens' fundamental rights and freedoms, particularly regarding personal data protection. It ensures that the exchange of personal data by competent authorities within the Union is not restricted due to data protection concerns. Additionally, it requires police agencies to appoint dedicated data administrators and grants citizens the right to access, manage, and delete their personal data processed or stored by the police. Furthermore, it mandates that each member state establish appropriate time limits for the erasure of personal data or periodic reviews of the need for data storage.

Spanish regulations comply with both *Regulation (EU) 2018/1139* and *Directive (EU) 2016/680*. Prior to these EU regulations, Spain had its own legislation governing drone use—*Royal Decree 552/2014*. With the implementation of the new EU acts, the Spanish Aviation Safety and Security Agency (AESA), operating under the EU's EASA framework, has become the primary regulatory body overseeing drone use in Spain. However, AESA primarily publishes information in Spanish, making access to information challenging. Additionally, the tests drone operators must take to fly in Spanish airspace are available only in Spanish. Despite these language barriers, Spanish laws fully comply with the new EU framework.

Similarly, as of December 31, 2020, Germany replaced its national drone regulations with the aforementioned European regulations. The German Federal Aviation Office (FAO), operating under the EASA framework, has confirmed adherence to the new EU regulations and that German regulations are now compliant with the updated European framework.

Poland has also implemented the new EU framework. The Polish Civil Aviation Authority (ULC), operating under EASA, maintains records of all registered drone pilots and can share this information with Polish police upon request. Polish law differs somewhat from other countries regarding surveillance competencies. Under the Polish *National Police Act*, the police have the authority to surveil all public spaces and private spaces during interventions. This broad authority allows Polish police to use any surveillance technology in their duties. This legislation is controversial, particularly because the ability to surveil private spaces during interventions was introduced simultaneously with *Directive (EU) 2016/680*, which aims to strengthen citizens' fundamental rights and freedoms. However, the *Directive* has at least regulated how long Polish police can store personal data—a previously unregulated and contentious issue. Police can now store personal data for a minimum of 30 days and a maximum of 60 days before deletion.

In the United Kingdom, the *Freedom of Information Act 2000* (FOIA) makes information regarding regulations, policies, and other acts readily accessible. FOIA also facilitates obtaining information from relevant authorities, making it easy to gather necessary details. Any surveillance data gathered, processed, or stored by British police is governed by the *Police Act*, the *Regulation of Investigatory Powers Act* (RIPA), and the *Protection of Freedoms Act* (PoFA). Additionally, British police must comply with the principles of the *Management of Police Information* (MoPI), which outlines issues that need consideration to comply with the law and manage risks associated with police information.

Perhaps the most crucial regulation is the requirement to adhere to the principles of the *Surveillance Camera Code of Practice* (SCCP). This mandates that police agencies create and follow a *Data Protection Impact Assessment* (DPIA) concerning the use of drones. While some paragraphs of this assessment are redacted and not publicly accessible, it is important to note that British police recognize the unique aerial perspective of drones, which may inadvertently capture members of the public near an operation. To minimize this risk, drone pilots are instructed not to record routinely unless they have a specific policing purpose.

3.2. In-depth interviews responses

The empirical study conducted in the United Kingdom, Germany, Spain, and Poland found that police drones are used relatively infrequently compared to the wide range of tasks typically performed by police officers. The two primary uses for drones are search and rescue operations and monitoring traffic. When questioned about other potential applications, such as city or crime scene mapping, monitoring public assemblies or protests, and regular CCTV-like surveillance, the responses varied. A German officer stated, “we wanted to, and we tried to monitor protests, but our [aviation] laws make it very difficult to perform such a task”. A Spanish officer noted that “during COVID-19, we used drones to urge people to stay home”, adding that “there is a unit that regularly monitors beaches”. In the United Kingdom, an officer mentioned, “we used drones to surveil cities during our pilot programs, but we rarely use them this way

³Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

anymore”, explaining that regular CCTV cameras usually provide sufficient information. Polish police “*mainly use drones for search and rescue operations due to the management’s approach*”. Polish police officer also stated that official statistics indicate that using a police drone in search and rescue operations can “*locate a missing person 191 seconds faster than teams without a drone*”.

All respondents noted that using a drone is quicker and cheaper than using a helicopter, and it appears that drones are consistently viewed as an alternative to helicopters rather than to technologies like CCTV cameras. It was emphasized that drones are intended to supplement helicopters, not replace them, by using drones as the initial response. Several respondents from different countries also highlighted few drawbacks of using drones. They mentioned the dependency on weather conditions: “*If it’s too windy, it won’t fly; if it rains, it won’t fly. Same with fog, too much sun, or extreme cold*”. Another issue was connectivity, which can be “*patchy*” in highly urbanized areas, hindering the officer’s live view on the screen and increasing the risk of crashes without proper precautions. Perhaps the most serious critique came from three respondents who felt that drones are not as useful as they are portrayed to the public (and police agencies). A British officer stated:

[...] it’s all just a gimmick. Sure, it’s nice to have a view from the air, but in most instances, what does that give us? It makes for a great PR stunt, but from my perspective, I have to prepare a flight plan, assemble the team, perform proper checks before the flight, and then make sure to properly store the data and draw up a report. There are few instances where drone missions have significant advantages over traditional policing.

In contrast, a Spanish officer stated, “*of course they [drones] are useful. Monitoring beaches is tiresome and takes a long time, and this saves us time and resources, including personnel*”. When asked about the bureaucracy surrounding drone missions, he replied, “*whether you go on a foot patrol or fly a drone, you have to write a report. What difference does it make?*”.

Regarding privacy concerns, respondents had mixed reactions. Generally, they acknowledged the importance of respecting privacy. A respondent from the UK noted, “*our regulations put citizens’ privacy first. We cannot simply fly the drone whenever we feel like it. We need to justify the flight, set a specific route, and assess privacy risks*”. A German officer added, “*citizens’ privacy and personal data are very important to us, and we try to minimize the data we gather to the bare minimum*”. In Poland, a respondent agreed that privacy is important, but when asked about instances of recording private property while monitoring traffic, seemed not to fully grasp the issue. A Polish officer confirmed the conclusion from doctrinal legal research, stating, “*there is no law against recording private property by accident while operating a drone during a legitimate task*”.

3.3. Results from field observations

On three occasions, permission was granted to observe actual police drone missions. The first observation took place in the UK, where a British officer demonstrated professionalism while explaining the necessary steps for the flight. Notes taken included: “*preparations similar to those done during civil flight – equipment check, map check, weather conditions check*”. Another note commented on the procedure: “*strict accordance to procedures; flight plan was set and executed; not allowed to speak with the officer during the flight; checks performed after flight; memo made after with appropriate form filled in*”.

The other two observations occurred in Poland, where police officers were monitoring traffic. In both instances, the drone operator sat in a car piloting the drone, while another officer stood near the road. When the operator identified a vehicle committing an offense such as illegal overtaking, reckless driving, or speeding, he informed the officer by the road, who then stopped the vehicle, informed the driver of the violation, and issued a ticket. In one case, the driver initially refused to accept the ticket and was shown a recording of the violation after a prolonged discussion.

Several notes were taken during these observations. It was noted that “*both officers are extremely professional; the drone operator focuses on the flight and speaks only when a traffic offense is spotted; the other officer is calm and forthcoming when informing drivers of their violations*”. Additionally, it was observed that “*the drone operator clearly knows what he’s doing, operates the drone perfectly and well within aviation laws*”. The first observation was near a busy road surrounded by open fields, while the second was near an area with several houses adjacent to the road. It was noted that “*the drone clearly records not only the road but also private property; people sitting in their gardens can be seen but are not the focus of the operator*”.

Conclusions from field observations validate earlier assumptions. Depending on the location, using drones to monitor traffic raises significant privacy concerns, as drones can inadvertently capture images and data from private properties near public roads, potentially infringing on individuals’ rights. Additionally, the effectiveness of drone surveillance is highly weather-dependent; high winds, rain, fog, and extreme temperatures can severely limit their capabilities. Connectivity issues in highly urbanized areas can also lead to intermittent data

transmission, hindering real-time monitoring and increasing the risk of operational failures. Furthermore, continuous surveillance of citizens poses legal and ethical challenges, fostering public mistrust and raising concerns about over-policing and potential abuse of power. Finally, integrating drone data with existing traffic monitoring systems presents technical and logistical challenges, necessitating robust infrastructure and data management protocols to ensure accuracy and reliability.

4. Discussion

The research, conducted through doctrinal legal research, in-depth interviews, and field observations, revealed significant inadequacies in both legislation and the dissemination of information and education to the public and local communities, especially in Poland. Drones should not be regarded merely as mobile CCTV cameras, as their aerial perspective allows police to observe private property, creating an imbalance in the relationship between police officers and citizens. Furthermore, the lack of transparency undermines police legitimacy. Police should inform the public about the purpose, intended uses, and potential benefits of police drones to improve overall perceptions of this technology (Koper et al., 2015, p. 249). Transparency and clear communication about when and why police drones might be used are crucial (p. 251). This was generally evident in the studied countries, with the possible exception of the United Kingdom, where current regulations facilitate public access to information and align more closely with community policing strategies.

Despite the increasing success of drone technology in police work, it remains a developing field, with regulations often struggling to keep pace with emerging innovations. The groundwork laid by the European Union's aviation laws and data protection directive offers significant opportunities for national legislators. This study demonstrates that member states like Spain and Germany have used this opportunity to implement key regulations that safeguard citizens' right to privacy while balancing police efficiency and accountability. These countries found the transition easier because their existing laws were already somewhat aligned with new EU regulations, and they had a history of developed privacy protection and police drone accountability legislation. Post-Brexit, the United Kingdom has taken a different path, yet its solutions still exemplify how to maintain police visibility and transparency. Although not perfect, UK laws provide an accessible framework for the purpose, limitations, and privacy impact assessments of police drone use.

Conversely, the current state of Polish legislation leaves much to be desired. Despite incorporating the EU's regulations into national laws, Poland's legislation did not address specific issues arising from the integration of drone technology into police work. Polish laws do not differentiate between a CCTV camera, a body-worn camera, and a drone. In this particular field, significant groundwork remains. To meet Western standards, a distinct police drone act should be adopted. This act should be based on best practices from other countries and should cover the types of operations police can use drones for, the purposes of these operations, how they are to be conducted and documented, and how privacy risks should be assessed. It should also require police to minimize these risks and ensure compliance with the regulations.

The integration of drones into police operations also necessitates a new form of police accountability to address the unique challenges and ethical concerns associated with this technology. Traditional oversight mechanisms are insufficient for managing the complexities introduced by drone surveillance, such as privacy violations, data security, and potential misuse. Comprehensive regulations and transparent policies must be established to govern the deployment and use of drones, ensuring they operate within legal bounds and respect citizens' rights. Independent oversight bodies should be empowered to monitor drone activities, investigate complaints, and enforce compliance with established standards. Additionally, clear guidelines on data retention, access, and sharing are essential to protect sensitive information and prevent unauthorized use. Public engagement and education on the legitimate uses and limits of police drones can further enhance trust and accountability, ensuring that this powerful tool is used responsibly and ethically in law enforcement.

There are several ways to achieve greater transparency and accountability in police drone use. Firstly, in the event of a monitored activity, a simple notice stating that a police drone will be used is insufficient. The notice should explain why the event will be monitored, what attendees can expect, and how this measure ensures their safety. Secondly, each police drone should be easily distinguishable from civilian drones, either through color, markings, or both, and should always be equipped with signalling lights to enhance visibility. Additionally, while providing an audio notice to nearby public that a police drone is in use is a reasonable idea, this notice should not be given without context. Simply stating that a drone is in use could be perceived as repressive. Instead, clear information must be provided to ensure that passers-by understand the reasoning behind the drone's use and its intended benefits for public safety.

From the start of this study, it was evident that British police excel in transparency and information dissemination regarding their drone operations, in compliance with regulations. It is common to find detailed records of police drone flights on their websites, including specific start and end times, the purpose of the flights, and the outcomes achieved. This approach minimizes doubt and suspicion that can arise with the widespread use of drone technology. Police agencies—just like Kent and Sussex police departments used to do — should be required to publicly disclose their drone usage policies, including the purpose of drone operations, the types of data collected, and the measures taken to protect privacy. Implementing robust oversight mechanisms, such as independent review boards and regular audits, can ensure that drone operations are conducted ethically and in compliance with legal standards.

Also worth addressing are the operational limitations of drones. They require ongoing technical improvements and specialized training for drone operators. Investing in advanced drone technologies that can withstand various weather conditions and ensuring robust connectivity can enhance the reliability of drone operations. Additionally, providing comprehensive training for drone operators on legal standards, ethical considerations, and technical skills is essential for conducting effective and responsible drone missions.

5. Conclusion

Balancing security and privacy in the use of police drones is a complex challenge that requires a multifaceted approach. Developing comprehensive legal frameworks, enhancing transparency and accountability, protecting data privacy and security, engaging with the public, and addressing technical limitations are critical steps in ensuring that police drone use aligns with democratic values and legal standards.

It is clear that further research on this topic is necessary. This study highlighted that the issue extends beyond privacy concerns; it relates to the broader context of how lawmakers institute policing and approach police accountability. Countries where the use of police drones is positively assessed tend to have a more holistic approach to law-making, whereas others do not. Future research should explore the effect of police drones on public perception of police. Although some research on this topic is emerging in the US, there is still a lack of comprehensive studies on police drone use within the EU (Sakiyama et al., 2017). Another area of interest is the differing levels of success and public praise between Polish police forces' use of drones, an unexpected finding that warrants further investigation.

Acknowledgements

This paper is an output of the science project *Police use of drones* funded by the National Science Centre, Poland, registry no. 2018/31/N/HS5/01999.

The author gratefully acknowledges the assistance of Prof. Janina Czapska in her supervision throughout this study.

References

- BBC (2014), France bans use of drones to police protests in Paris. [Online] <https://www.bbc.com/news/world-europe-55411695>(May 20, 2024).
- Bennett-Moses, L., & Chan, J. (2014). Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools. *University of New South Wales Law Journal*, vol. 37(2), pp. 643-678.
- Bowman, J. (2014), Ontario police defend use of drone cameras over protests. [Online]<http://www.cbc.ca/newsblogs/yourcommunity/2014/03/ontario-police-defend-use-of-drone-cameras-over-protests.html> (May 20, 2024).
- Brighenti, A. (2007). Visibility: A Category for the Social Sciences. *Current Sociology*, vol. 55(3), pp. 323-342.
- Chynoweth, P. (2008). Legal Research. In A. Knight, L. Ruddock (Eds.), *Advanced Research Methods in the Built Environment* (pp. 28-39). New Jersey: Wiley-Blackwell.
- Hutchinson, T., & Duncan, N. (2012). Defining and Describing What We Do: Doctrinal Legal Research. *Deakin Law Review*, vol. 17(1), pp. 83-119.
- Koper, Ch., Lum, C., Willis, J., Woods, D., & Hibdon, J. (2015), Realizing the potential of technology in policing (Grant No. 2010-MU-MU-0019). [Online] <https://cebcp.org/wp-content/technology/ImpactTechnologyFinalReport.pdf> (May 25, 2024).
- Pearce, D., Campbell, E., & Hardin, D. (1987). *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission*. Canberra: Australian Government Publishing Service. Cited in: Hutchinson, T. (2018). *Researching and Writing in Law*. (4th ed.). Canberra: Thomson Reuters.
- Sakiyama, M., Miethe, T., Lieberman, J.D., Heen, M., & Tuttle, O. (2017). Big hover or big brother? Public attitudes about drone usage in domestic policing activities. *Security Journal*, vol. 30(4), pp. 1027–1044.