Privacy's sky-high battle: the use of Unmanned Aircraft Systems for law enforcement in the European Union

Kurtpinar, E.O.

Journal of Intelligent & Robotic Systems (2024) 110:99
https://doi.org/10.1007/s10846-024-02071-w

REGULAR PAPER

Privacy's Sky-High Battle: The Use of Unmanned Aircraft Systems for Law Enforcement in the European Union

E. Öykü Kurtpınar[1]

Received: 4 December 2023 / Accepted: 9 February 2024 / Published online: 9 July 2024

Abstract
Benefiting from the rapid advancements in Unmanned Aircraft Systems (UAS) technology with enhanced tracking and data collection capabilities, law enforcement authorities re-discovered air as a dimension where state power can be exercised in a more affordable, accessible, and compact way. On the other hand, during law enforcement operations, UAS can collect various types of data that can be personal or sensitive, threatening the right to privacy and data protection of the data subjects. Risks include challenges related to data security, bulk data collection, the diminished transparency and fairness resulting from the inconspicuous nature of UAS, as well as ethical concerns intertwined with privacy and data protection. Upon examination of the legal framework including the General Data Protection Regulation the Law Enforcement Directive, various Aviation rules, and the new proposal for the Artificial Intelligence Act, it becomes apparent that the EU legal framework's adequacy in safeguarding privacy and data protection against law enforcement use of UAS is context-dependent, varying across use cases. The current framework lacks clarity, leading to arbitrary application and limited protection for data subjects. Enforcement of safeguards is insufficient, and the Aviation Regulations, applicable to law enforcement UAS, require member states' opt-in, which has not occurred as of the authors' knowledge. The Artificial Intelligence Act addresses UAS operations but focuses on market risks rather than obligations imposed on law enforcement authorities. Consequently, the existing framework is rendered inadequate for medium to high-risk law enforcement operations, leaving individuals vulnerable and insufficiently protected against intrusive UAS surveillance. Rectifying this involves addressing the enforcement gap and making the necessary amendments to relevant regulatory aspects. Additionally, the implementation of specific technical measures and steps to foster effective cooperation among stakeholders in UAS deployment for law enforcement is imperative.

Keywords Law enforcement · Privacy · UAS (Drone) · GDPR

1 Introduction

Unmanned Aircraft Systems (UAS), commonly known as 'drones', have evolved to serve various purposes today, ranging from recreational uses to commercial applications such as agricultural monitoring, scientific research, fimmaking and cargo delivery [1]. Law enforcement authorities (LEAs) too, have increasingly adopted UAS, benefitting from their portability, enhanced video and photography capabilities, and diverse functions in response to evolving means and definitions of crime.[1]

Law enforcement mainly concerns coercing compliance with the laws. Its models differ among states, such as public police service [3] customs and border protection [4], intelligence services [5] or investigative bodies. The European Union (EU)'s competence to regulate law enforcement is limited, as it primarily is within the jurisdiction of individual Member States. Nonetheless, especially after the Lisbon Treaty abolished the three-pillar structure, the EU increasingly regulates law enforcement matters, albeit based on its competence on fundamental rights, including data protection and privacy [6].

The technicalities of UAS can be custom chosen to accommodate different purposes and operational needs LEAs encounter. Observing the most common UAS models deployed by the LEAs, such as "DJI's Mavic 2" or

✉ E. Öykü Kurtpınar
e.o.kurtpinar@law.leidenuniv.nl

[1] Institute of Air and Space Law, Leiden University, Leiden, Netherlands

[1] For the difference between "cyber-enabled crimes" and "cyber dependent crime", *see* Wagen and Oerlemans [2].

"Avy Dock", they can range from small handheld drones to medium-sized or large drones, fixed-wing drones to multi-rotor drones. They might be lightweight and compact, weighing less than 1 kg [7], or heavier, weighing over 10 kg [8]. Having different transmission distances from 1 to 200 km, they can resist wind and travel at maximum cruising speeds of up to 90 km/h [9]. Flight time depends on various factors such as weather conditions, the type of drone,[2] flight weight, or battery operation temperature. While a standard law enforcement drone can stay in the air for 20–30 min [10], high-end police drones can fly for a few hours such as Hybrix Long-Endurance Drones [8].

While the LEAs' connection with the air precedes UAS with helicopters, UAS allowed LEAs to re-discover air as a power dimension in an affordable and user-friendly nature where a "*perspective from which policing can be carried out*" [11] and implement new services while significantly reducing the risks for law enforcement officers [12].

Equipped with cameras, sensors, and speakers, UAS enable successful task execution in inaccessible locations [13]. They offer distinct advantages over traditional surveillance methods, such as CCTVs or bodycams with their tracking capabilities, aerial view, ability to modify their functionality through various payloads, and relatively lower costs as compared to manned aircraft such as helicopters. These enable LEAs to conduct different operations for law enforcement and surveillance, civil protection, and regulatory enforcement [14].

Law enforcement and surveillance purposes for which UAS are used, include monitoring hotspots, controlling crowds during protests [15] and riots[16], or festivals[17], with the latest example of the French UAS deployment against the 2023 Paris riots[18]. UAS are used also for enforcing quarantine measures [19] or targeted criminal investigations[20]. For these objectives, different payloads such as thermal and smart cameras are used to capture, store, and stream diverse data while also enabling LEAs to identify human or animal density and detect individuals carrying guns among the crowd [21, 22].

Other uses include transferring communications and warnings [23], carrying and dispersing pepper sprays (a practice already exercised in India) [24], and supporting police response operations with its various payloads such as beacons [24], Global Positioning Systems (GPS), night vision[25], or radio frequency equipment that can identify mobile signals and intercept phone conversations and internet activity[26].

Controversial yet feasible, UAS can incorporate software payloads like facial recognition [27] and "*smart surveillance*" [28] systems. These capabilities enable LEAs to identify and profile specific individuals or objects [29] and detect abnormal or anti-social behaviour for early crime detection [30]. Other less controversial uses of UAS include collecting 3D and 4D crime scene photos [31] and infrastructure protection against theft [32].

Besides law enforcement and surveillance, UAS are used also for civil protection (e.g., search and rescue missions, monitoring of critical infrastructure) and regulatory enforcement (e.g., mapping and earth observation). These operations pose relatively lower risks as they focus mainly on landscapes rather than individuals, making collecting personal data less likely [14].

During these operations, various data are collected. Advanced surveillance technologies, such as facial recognition software and algorithmic tools, broaden the range of data, further including identity and behavioural data. This includes non-neural contextual information, such as voice, written text, and facial images, which are used to infer mental processes or obtain biometric data [33].

Table 1 [14] briefly indicates LEAs' UAS operations and various types of data collected (e.g., visual, audio, geolocation, behavioural, and biometric data) during these operations.

In the face of these data collection activities of UAS, the widespread use of UAS, including its controversial application during the COVID-19 pandemic [34], has resurfaced concerns, especially on the right to privacy and data protection, despite its capabilities and advantages. Nonetheless, the objective of this article is not to propagate a dystopian narrative surrounding the legal concerns over UAS use. Instead, it aims to thoroughly analyse the potential risks associated with UAS use of LEAs and develop precise policy recommendations promoting responsible and beneficial implementation. For that purpose, it is necessary to examine the adequacy of the applicable EU legal framework surrounding the UAS use of the LEAs. There exists a fragmented legal framework for privacy and data protection aspects of UAS operations, which consist of privacy, aviation, and artificial intelligence (AI) legislations.

2 Privacy Law

Although it may not fully resolve collective issues such as discrimination or the erosion of democracy and civil rights, safeguarding privacy and data protection stands as a crucial initial step in addressing broader concerns, such as cybersecurity, safety, civil liberties and due process. Therefore, specific examination of LEAs' UAS, using a privacy and data protection lens, is essential.

From a dimensional privacy perspective [35], UAS operations infringe upon the following:

[2] For instance, a fixed-wing drone can endure flight times longer than a multirotor drone.

Table 1 Types of UAS operations in law enforcement context, payloads used and data collection activities

Mission	Operation	Payloads	Target	Data Collected
Law Enforcement and Surveillane of people	-Monitoring hotspots -Controlling crowds (during protests and riots or festivals) -Monitoring -Enforcing quarantine measures -Criminal investigations -Detection of abnormal or anti-social behavior -Early crime detection -Police response -Infrastructure protection against theft	-High-Resolution cameras -Thermal Cameras -Audio Recording -Facial Recognition Systems -Smart Surveillance Systems (Biometric and Behavior Identification Software) -Loudspeakers -Beacons -GPS Tracking Systems -Night Vision -Radio Frequency Equipment -Wi-Fi Sniffers	People	**Personal and sensitive data** -Image, audio, vedio, thermal, or geolocation data -Mobile phone signals, phone conversations, text messages, and internet activity -Identify or behavioral data
Civil Protection	-Emergency planning and response -Surveillance of critical infrastructure -Search and rescue missions -Firefighting -Monitoring environmental, biological, and chemical hazards	-High-Resolution cameras -Thermal Cameras -GPS Tracking Systems -Loudspeakers -Radio Frequency Equipment (Mobile Phone Sensors) -Audio Recording -Sample Collector Sensors	Landscapes, People	Focus is mostly on landscapes, **collection of personal or sensitive data is less likely** -Geolocation data (e.g., Mobile phone signals) -Image, audio, video, thermal
Regulatory Enforcement	-Enforcement of sector-specific rules and regulations -Monitoring pollution and illegal logging etc. Activities -Mapping and earth observation	-High-Resolution Cameras -Thermal cameras -GPS Tracking Systems -Sample Collector Sensors	Landscapes, People	Focus mostly on landscapes, **collection of personal or sensitive data is less likely** -Image, audio, video, thermal, or geolocation data

i.Physical privacy encompasses "spatial seclusion and solitude" involves bodily and territorial aspects. UAS can track and identify individuals with thermal or high-resolution cameras and record their voices with microphones, firstly violating bodily privacy. Territorially, UAS can also fly over private properties, including homes and workplaces, where observation is not expected.[3] With advanced imaging capabilities, UAS can surveil private spaces by seeing through walls and windows, providing law enforcement with a unique surveillance perspective beyond traditional methods.

ii.Social (interactional) privacy can also be infringed through UAS international mobile subscriber identity international mobile subscriber identity (IMSI) trackers or surveillance software, intercepting mobile signals, remotely disabling phones, and recording conversations and social interactions using microphones during crowd control operations [26].

iii.Psychological privacy as the feeling of constant surveillance by UAS can induce psychological effects like paranoia, heightened stress levels, self-censorship, and behavioural modifications to project compliance.

iv.Informational privacy since UAS can collect various types of data in massive volumes, which in nature could be personal[4] or sensitive[5] (see Table 1.), revealing private aspects of individuals' lives.

The General Data Protection Regulation (GDPR) [33] and Law Enforcement Directive (LED) [36] are the two primary EU-level privacy legislations applicable to UAS operations. They share certain principles, terminology, and safeguards, yet they differ in some substantial aspects, including the level of protection they afford to individuals.

[3] For the Dutch DPA report *see* [36].

[4] Personal data is defined as "any information relating to an identified or identifiable natural person", GDPR art 4(1).

[5] GDPR, art 9.

2.1 Boundaries of Material Scope Between Law Enforcement Directive and GDPR

The varying safeguards and levels of protection for different UAS operations necessitate clarifying the demarcation of scope between LED and GDPR. GDPR's material scope includes the processing of personal data by wholly or partially automated means.[6] However, certain activities are excluded from GDPR's scope, such as the processing by competent authorities for the *"prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"*.[7] These processing activities are regulated under the parallel, *lex specialis* LED,[8]setting law enforcement-specific rules for personal data processing [38]. However, determining the precise boundaries between the GDPR and LED is complex, as highlighted by scholars and the European Commission Expert Group [39, 40].

LEAs conducting UAS operations, such as police and investigative bodies, possess the required competence for the first criterion of the LED's scope: processing by the "*competent authority*" [41]. Regarding the material criteria, processing purposes under the material scope of LED and their respective UAS applications are;

i. **Prevention of criminal offences:** Includes UAS operations aimed at anticipatory action to prevent future crimes,[9] such as monitoring hotspots, crowd controls, quarantine measures, detecting abnormal or antisocial behaviours, and early crime detection. Most of the UAS operations described under law enforcement and surveillance,[10] fall under this purpose.
ii. **Investigation, detection, or prosecution of criminal offences and execution of criminal penalties:** These encompass UAS operations that are reactive responses of the state to the crime committed. Examples include crime scene mapping, searching for deceased individuals, forensic investigations [42], police response operations (e.g., hostage situations) [43], and detecting violations of quarantine measures.

Member States can influence the scope of the LED, as detailed formulations for investigation, detection, or prosecution are provided under domestic laws rather than the LED. This may potentially change the applicable legal framework for UAS operations [41].

The LED's formulation of "*prevention"* and *"criminal offences"* creates uncertainty over its scope, leading to inconsistent interpretations, legal uncertainty, and the potential for arbitrary application. This poses a risk to data protection and privacy, degrading the protection afforded to individuals.

For the term "*criminal offence",* the European Commission's Legal Service attempted to clarify its ambiguity by allowing Member States to rely on their domestic definitions of "*criminal offence"* instead of a harmonised EU criteria [39]. This new approach addresses discussions about processing personal data for different crime categories, such as minor crimes or administrative offences, which may be distinguished from criminal offences in certain legal systems [41]. Consequently, LEAs who might lack strong legal expertise must identify the classification of specific crimes (investigated or prevented using UAS) to determine the applicable privacy legislation and their obligations. This may also arbitrarily expand the LED's scope of application to UAS operations and cause scope inconsistencies among member states [41].

The added phrase in the LED, *"safeguarding against and the prevention of threats to public security",* along with *"threats to fundamental societal interests with future crime potential"* (underlined in recital 12), expands Member States' discretion. Departing from traditional law enforcement purposes, this expands LED's application to predictive and preventive policing.[11] Overall, general ambiguity may put UAS operations unrelated to the objective of the LED under its scope [46].

2.2 GDPR v. LED, Common Principles and Differences

The LED and GDPR aim to protect fundamental rights, including personal data protection, and facilitate data flow among EU authorities.[12] However, the LED provides contextualised and balanced protection to accommodate the needs of LEAs and individuals' data protection simultaneously[38]. Both legislations emphasise fair principles for processing personal data and the rights of data subjects, promoting *"informational self-determination."*[13] Nonetheless, UAS operations present specific challenges to these safeguards.

[6] GDPR, art 2.

[7] GDPR, art 2 (2) (d).

[8] LED, art 1–2.

[9] *See* Welsh and Farrington in 'Crime Prevention and Public Policy' [44].

[10] *See* Table 1.

[11] For guidance of the French Data Protection Authority *see* [45].

[12] LED, art 1.

[13] Concept of informational self-determination is deemed problematic within the context of the LED by some authors. *See* Leiser and Custers in [38] 369.

2.2.1 Data Protection Principles

By examining the application of data protection principles outlined in both legislations, this section aims to illuminate the distinct protections offered by the LED and GDPR and explore how UAS, as an emerging technology, can both align with and challenge the application of these data protection principles in the law enforcement context.

a. Lawfulness, Fairness and Transparency

Data processing during UAS operations should be lawful and fair under both legislations [38]. For UAS operations under the LED, such as crowd control, LEAs cannot rely on the prior consent of the subjects, which cannot be given genuinely and freely.[14] The only lawful ground under the LED is the "*necessity of for the performance of the tasks"* of the competent authority.[15] Nevertheless, data subjects can voluntarily agree on the processing of their personal data, albeit not making the processing lawful [47].

For UAS operations under the GDPR, LEAs must obtain free and informed consent unless they rely on other applicable grounds.[16] Assuming implicit consent by individuals in public areas under UAS surveillance due to lower expectations of privacy, contradicts the GDPR and LED's emphasis on informational self-determination. Besides, the visible invisibility of UAS operations poses challenges to the criteria for valid consent that is "*informed*" and "*unambiguous*", whereas UAS bulk data collection capabilities complicate consent being "*specific*".

LEAs must inform individuals about the risks, regulations, safeguards, and rights associated with UAS operations and data collection for data processing, as mandated by the principle of fairness, which is intrinsically related to transparency.[17] Nevertheless, UAS operations under the LED have lower transparency requirements than under the GDPR[18] to preserve the effectiveness of ongoing criminal investigations [38] and "*covert investigations or video surveillance"*.[19]

It is uncertain to which level LEAs can inform individuals on the abovementioned rights and risks during, before, or after UAS operations due to the technical complexity and visible invisibility of UAS operations. The characteristics of UAS, including their small and stealthy design, make it difficult for data subjects to fully comprehend the data collection and processing activities, creating a visible invisibility [48]. Even if subjects are aware of the UAS flight, it is often unclear the sensors and payloads used, the collecting authority, the data being collected, and the intended purposes [49].

b. Purpose specification and limitation

The purposes for which UAS collect and process data must be specific, explicit, legitimate, and defined before the processing under both legislations.[20] Further processing must occur for the initially specified (or compatible) purposes.[21] However, for UAS applications under the LED, processing for additional purposes is permitted if it falls within the LED's scope, is necessary, proportionate, and authorised by relevant legal provisions.[22] Therefore, problematically, UAS data collected for searching youth groups in principle can also be used to identify suspected marijuana cultivation areas [14].

On the other hand, there are significant challenges to the practical application of this principle. UAS, due to their mobility, collect data in bulk amounts [29] and indiscriminately without distinguishing objects or individuals. These operations might have unspecified "*general surveillance*" purposes, and missions' objectives may change during the flight. Different terms, including "*big drone data*", highlight the risk of "*fishing expeditions"* where past collected data is used for non-predetermined purposes *and ex post facto* law enforcement [50]. Thus, there are insufficient legal safeguards for purpose-specific data collection for UAS operations, especially under the LED.

c. Data Minimisation

Personal data collection and processing by UAS should be; limited to i. "*what is necessary"* for the legitimate purpose ii. "*proportionate*", and iii. "*not substitutable by less invasive means"*.[23]

Firstly, unless privacy-enhancing technologies are used, UAS' extensive breadth of view collects bulk amounts of undifferentiated data not strictly necessary for LEA's specific purposes. The second and third requirements are also problematic, as the effectiveness and necessity of UAS deployment are often uncertain, as seen in the criticised use of UAS for enforcing COVID-19 measures [14]. Additionally,

[14] LED, art 8.

[15] LED, art 8.

[16] Other two grounds LEA can rely on for their UAS operations are protecting "the vital interests of the data subject or of another natural person" or "necessary for the performance of a task carried out in the public interest", GDPR art 6(1)(d)-6(1)(e).

[17] LED, rec 26; GDPR rec 39.

[18] GDPR, 5(1)(a).

[19] LED, rec 26.

[20] LED, art 4 (1)(b); GDPR art 5 (1)(b).

[21] LED. rec 26.

[22] LED, rec 29.

[23] LED, art 4 (1)(c); GDPR, art 5(1)(c).

tasks that could be handled by less intrusive methods like CCTV and bodycams (e.g., monitoring public gatherings) are increasingly assigned to UAS.

Technical and organisation restrictions, (already enacted in certain Member States[24]) and specific guidance from DPAs are often seen as safeguards against indiscriminate bulk data collection complementing the GDPR and LED. Nevertheless, concerns about the practical implementation of these limitations due to officers' potential lack of expertise and awareness of legal constraints persist.

d. Data Security

Against the inherent risks carried by UAS operations, such as the Wi-Fi connection of UAS for transmitting data, hijacking [52], or hacking [53] both legislations mandate state-of-the-art measures. For instance, using a publicly available source code or deceptive GPS signals, attackers can deploy another UAS as a Wi-Fi Sniffer and hijack law enforcement UAS to create "*an army of zombie drones*" [52]. Both legislations aim to prevent unauthorised processing, accidental loss, destruction, or damage of data,[25] including pseudonymisation and strong encryption of UAS data.[26] The LED also introduces "*logging*"[27] to mitigate data and security breaches and monitor unlawful processing, staff activities, and unauthorised access [47].

For UAS using third-country servers, data transfers shall take place only to the third countries with an "*essentially equal"* level of protection of rights and freedoms to prevent potential data leaks to foreign public and private authorities [38].[28] This can be shown by the Commission's legally binding adequacy decisions, or the controller demonstrating appropriate safeguards. Despite numerous adequacy decisions for the GDPR,[29] in the absence of adequacy decisions for data exchanges in the law enforcement sector,[30] third-country transfers for LEAs' UAS occur without sufficient safeguards and data security [56]. Even when the data transits through third countries without constituting a third-country transfer, additional measures and safeguards are necessary to safeguard the data security. These risks significantly undermine data protection rights, necessitating regulations mandating EU-based servers for UAS data or effective enforcement of third-country transfer rules.

e. Data Accuracy

UAS data must be accurate, up to date, and rectified or erased without delay if found to be inaccurate.[31] However, the technical capabilities of UAS and payloads may undermine this principle. Factors such as limited field of view, adverse weather conditions, operator errors, and sensor limitations can lead to the UAS collection of inaccurate data. Additionally, algorithms used for preventive and predictive policing on UAS have an inherent error rate, resulting in the creation of inaccurate personal data.

f. Sensitive Data Collection

UAS collection of sensitive data poses an even higher risk to the rights and freedoms of data subjects [57]. It increases the likelihood of discrimination and harm to vulnerable groups and individuals.[32] In line with the GDPR and LED definition of sensitive data, UAS can collect:

- *"Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs"* or *"data concerning a person's sex life or sexual orientation":* Identification of individuals with UAS during crowd control operations such as political protests, religious meetings, trade-union strikes, or pride parades, reveals affiliations with politics, religion, and sexual/racial identities.
- *"Genetic data, biometric data processed solely to identify a human being":* Data analytics payloads enable the collection of such sensitive data through face recognition, gait analysis, and biometric identification software. However, these technologies are prone to biases, errors, and false positives that can elevate the severity of unjust outcomes.
- *"Health-related data":* UAS can detect fever or elevated body temperature as an indicator of illness using thermal imaging cameras, as in the recent instance of the COVID-19 pandemic [58].

UAS' enhanced data collection capabilities and payloads with data analytics tools contribute to the evolution of sensitive data. More personal data becomes sensitive based on its context of use [59, 60]. By combining various data sets under their control, LEAs can increasingly draw sensitive

[24] For the examples in CNIL, *see* Opinion on a draft decree implementing Articles L. 242–1[51].

[25] LED, art 4(1)(f), 29; GDPR 5(1)(f).

[26] LED, art 4(1)(f), 29; GDPR 5(1)(f).

[27] LED, art 25.

[28] *See* 3rd country transfer rule, Schermer in 'The Limits of Privacy in Automated Profiling and Data Mining' [54].

[29] *E.g.* Andorra, Argentina, Israel, Japan, Switzerland, United Kingdom.

[30] Currently, no adequacy decisions to a country other than United Kingdom is recognized for data exchanges in the law enforcement sector [55].

[31] GDPR, art 5(1)(d), LED, art 4(1)(d).

[32] GDPR, rec 71.

Table 2 Overview of data subject rights in the Directive 2016/680 and GDPR

Data subject right	Directive 2016/680	GDPR
Right to information	Articles 12–14	Articles 12–14
Right to access	Articles 14–15	Articles 15
Right to rectification	Article 16	Articles 16
Right to erasure (right to be forgotten)	Article 16	Articles 17
Right to restriction of processing	Article 16	Articles 18
Right to data portability	N/A	Articles 20
Right to object to automated individual decision-making	N/A	Articles 21–22

conclusions. For example, UAS surveillance in residential areas may capture non-sensitive data about individual's activities. Still, when combined with other sources, it may reveal sensitive characteristics and lead to discriminative profiling.

For UAS operations outside the criminal context, such as emergency response, the GDPR establishes a general prohibition on sensitive data processing, subject to exceptions.[33] However, for UAS surveillance operations under the LED, less protection is afforded since the processing of sensitive data is allowed but with the conditions of being strictly necessary and subject to appropriate safeguards.[34] Nevertheless, Article 29 Working Party (WP29), predecessor to the European Data Protection Board, recognising the higher risk posed by LEA's sensitive data processing, suggests conducting a DPIA and introducing additional safeguards such as prior judicial authorisation, higher security standards, and access authorisation requirements [46, 47].

Two primary concerns arise for the application of these GDPR and LED rules. Firstly, the basic UAS data collection capabilities lack the technical means to automatically distinguish sensitive data from personal data (unless additional algorithmic tools are deployed). Also, implementing filtering mechanisms for sensitive data necessitates sensitive data processing in the first place. For instance, UAS crowd control operations during Ramadan celebrations may unintendedly and illegitimately collect religious data without sustaining "*strictly necessary*" criteria, as it cannot be separated from other personal data.

Secondly, the data collected by UAS, even if it does not strictly fall under the narrow categories of sensitive data, can still result in discrimination or similar harms due to the broadening of sensitive data concepts. Therefore, the GDPR and LED fail to adequately address the expanding scope of "*sensitive*" information and evolving data collection methods used by UAS and surveillance technologies.

2.2.2 Data Subject Rights

Data subject rights (*see* Table 2*)* are essential safeguards against privacy-invasive UAS operations. They are described more in detail in the LED as compared to the GDPR's general descriptions [40].

i. Right to information and access:

LEAs' UAS operations under the GDPR (e.g., civil protection, search and rescue) must inform data subjects about processing purposes, means, risks, safeguards, and data subject rights.[35]

For UAS operations under the LED, requirements are differentiated as *"making information publicly available*" (e.g., controller identity, processing purpose) and providing specific information (e.g., legal basis, data storage period).[36] This two-folded informational obligation may partially mitigate LED's lower transparency requirements.

ii. Right Rectification and Erasure and Restriction of Processing:

If inaccurate UAS data collection or processing occurs, subjects can obtain rectification or erasure rights under both the GDPR and LED.[37] Conditions for restrictions are formulated differently, with the LED providing more vague formulations (e.g., for "*protecting public security"*).[38]

Restrictions on data subject rights in the law enforcement context are reasonable to avoid hindering criminal investigations. However, their formulations are vague, especially within the LED, such as (for access rights) to avoid obstruction, prejudice investigations, and protect public/national security and the rights of others,[39] or (for rectification and erasure) "*protecting public security"*.[40] Nonetheless, the exercise of these rights and legal certainty are particularly essential in the law enforcement context where the risks of processing inaccurate UAS data is elevated, particularly as evidence in court proceedings [46]. Besides, data subject rights are often hindered by the limited awareness of UAS data collection activities and the collector's identity,

[33] GDPR, art 9.

[34] LED, art 10.

[35] GDPR, art 13, rec 39.

[36] LED, art 13(2).

[37] LED, art 16 (1)-(3); GDPR, art 16–18.

[38] LED, art 16(3); GDPR, art 17(3).

[39] LED art 15.

[40] LED, art 16(3); GDPR, art 17(3).

especially when small UAS operate silently and inconspicuously at high altitudes [14].

2.2.3 Automated Individual Decision-Making

UAS operations with the purpose of preventive policing [61] may incorporate AI into aerial surveillance [62]. This incorporation offers valuable surveillance capabilities, including facial recognition,[41] real-time violence detection,[42] and temporal anomaly detection.[43] Other big data sources and external Internet of Things (IoT) information can be effectively combined with UAS data through AI and cloud data management forms (*i.e.,* Internet of Drones) to increase the scale and efficiency of "*smart city surveillance*"[66]. In the future, UAS-based fully automated decisions, regulated under the LED and GDPR, for predictive and preventive policing is technically possible.[44]

Besides the criticisms presented by the scholars towards the concept of preventive policing [67], in a future scenario where UAS replace law enforcement officers, the asymmetrical interaction between humans and machines may also contribute to dehumanising both the observer (LEAs) and the observed [68]. LEAs may reduce citizens to data points of 'good' or 'criminal', while citizens oversimplify LEAs as mechanical entities lacking empathy, discretion, and nuanced decision-making.

AI-incorporated UAS surveillance operations primarily fall under the LED, but domestic laws may invoke the GDPR, such as for UAS surveillance related to minor offences. Rather than imposing a prohibition, GDPR provides individuals the right to object to solely automated decision-making.[45] Under the LED (e.g., predictive policing), these decisions, with a specific emphasis on the ones using sensitive data, are prohibited in principle.[46] However, provisions' exceptions raise doubts about the prohibition's effectiveness and require more elaborate guidance.

Current UAS profiling and surveillance operations involve human oversight, unless fully autonomous UAS with their own decision-making and executing capabilities are deployed [69]. Accordingly, LEAs using these fully automated UAS, although technically feasible, would be non-compliant under the current legislation.

2.2.4 Data Protection Impact Assessment (DPIA)

DPIAs safeguard privacy and data rights by increasing transparency, prompting LEAs to proactively consider UAS' risks and identify mitigation measures while using a fundamental rights lens [70].[47] They also serve as tools to demonstrate legal compliance, thus enhancing public acceptance of UAS.

For UAS operations under the LED, LEAs, as an agency who is the operator and the data controller, must conduct a DPIA when the activity is likely to pose a high risk to individuals' rights and freedoms, taking into account "*the nature, scope, context, and purposes of the processing*".[48] However, under the GDPR, a non-exhaustive list of circumstances is provided to determine when a DPIA is required.[49] Thus, LEAs are not obligated to conduct a DPIA for every UAS processing activity (e.g., search and rescue operations). However, it is advised to conduct separate DPIAs before deploying UAS and payloads, even when not strictly required, considering LEAs' general obligation for adequate risk management [70].[50]

2.2.5 Privacy by Design (PbD) Requirement

PbD methodology, provided under both legislations, accommodates legitimate interests in a positive-sum manner, allowing security and privacy to coexist in UAS operations. Accordingly, LEAs as data controllers must integrate privacy considerations and safeguards into their UAS design and architecture from the outset[51] in which data protection principles become a part of UAS functioning [71].

PbD encompasses not only technical aspects but also organisational measures, ensuring that law enforcement's procedure for UAS use is privacy-preserving. Hence, legally imposing the PbD approach on LEAs can significantly improve the deficiencies of UAS operations regarding data protection principles.

3 Aviation Law

Aviation legislation and EASA's competencies traditionally and primarily concern aircraft safety[1]. Regulation 2018/1139 (Basic Regulation) is an aviation safety regulation based on TFEU 100(2) without the primary authority to address privacy concerns, similar to EASA and drone rules [72]. Nevertheless, it explicitly includes contributing

[41] *See* as an example [63].
[42] *See* as an example [64]
[43] *See* as an example [65].
[44] LED, art 11; GDPR, art 22.
[45] GDPR, art 22.
[46] LED, art 11.
[47] LED, art 27; GDPR, art 35.
[48] LED, art 27, rec 53.
[49] GDPR, art 35, rec 91.
[50] LED, 19(1).
[51] LED, art 20, GDPR, art 25.

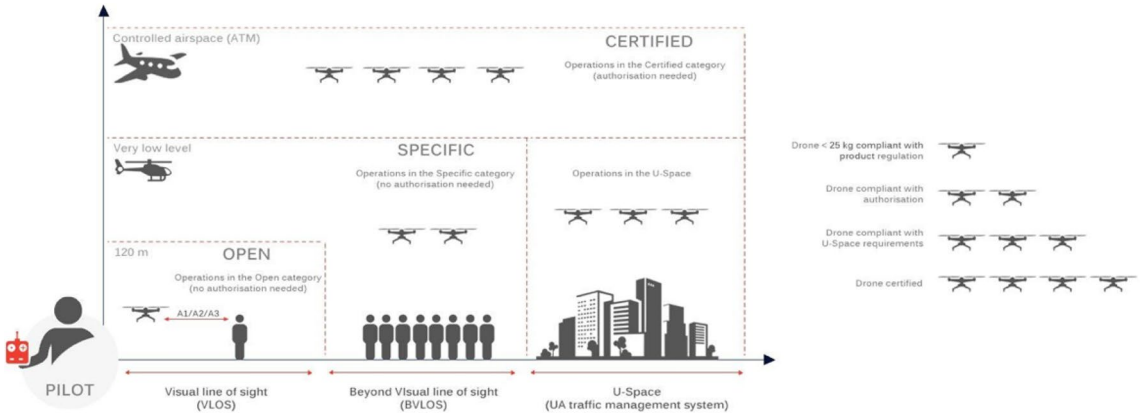

Fig. 1 Risk-based categorisation of UAS operations

to privacy and data protection among its objectives and addresses privacy as a secondary matter interlinked with safety [73].

EU aviation rules offer valuable insights into privacy and data protection concerns. However, principally they are not applicable to LEAs' UAS as they fall under 'State' flights according to the Basic EASA Regulation classification [74].[52] Nevertheless, these rules should still be examined in this thesis since an option for Member States to opt-in for the applicability of Regulations 2018/1139, 2019/947 and 2019/945 to their state aircraft is provided.[53] Thus, the examination of the following aviation rules assumes the scenario where opt-in is preferred by the member states.

Firstly, Regulation 2018/1139imposes obligations regarding UAS posing privacy and data protection risks and their operators (LEAs) to be registered, identified, and individually marked [74]. These requirements mitigate, to a certain extent, accountability, fairness and transparency of UAS operations.

Secondly, the Regulation 2019/947 [76] requires UAS to conduct DPIAs[54] and adopt privacy-by-design measures[55] similar to the GDPR and LED. Recommended examples include e-identification and geo-awareness (to assist remote pilots in complying with areal restrictions) [76]. This can promote the market adoption and prevalence of UAS with privacy-friendly features, thereby indirectly influencing LEAs' purchasing preferences. Moreover, the Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Regulation (EU) 2019/947 [77], provide that additional guidance material for operators to identify and mitigate privacy and data protection risks should be provided by the competent authorities [79].

Detailed under Regulation 2019/947, Member States can "*facilitate, restrict or exclude"* UAS operations within a portion of airspace,[56] and "*allow access only to UAS equipped with certain technical features"*.[57] For instance, geographically restricting LEAs' usage of UAS equipped with high-resolution cameras within residential areas can prevent image data collection from inside the individuals' homes. Promoting proportionality, data minimisation, and purpose limitation, geographical restrictions can practically remedy privacy impacts. However, concerns arise regarding the regulatory flexibility in defining UAS geographical zones and the competence of the authority assigning geographical zones on privacy-related matters, given its primary expertise in aviation [80].

The necessity of ensuring all drone services are provided in a privacy-friendly manner aligned with the anticipations and the concerns of the citizens is underlined in the Commission's recent *"Drone Strategy 2.0"*[80]. The strategy emphasizes the necessity of secondary considerations, including privacy, so that UAS can be considered as "*an instrument of a more significant project"* [81].

As shown in the Fig. 1 [82] Regulations 2019/947 and 2019/945 [83] adopt a risk-based approach while categorising UAS operations as 'open,' 'specific and 'certified'[58]

[52] The Regulation defines a flight, a "state flight" when it is conducted "under the control and responsibility of a Member State, undertaken in the public interest by or on behalf of a body vested with the powers of a public authority" during the activities of, but not limited to, "military, customs, police, search and rescue, firefighting, border control, coastguard". Any aircraft not falling under "state" is a "civil aircraft"; Regulation 2018/1139, art 2(3)a; see also Masutti and Tomasello [75], 52.

[53] Regulation 2018/1139, art 2(3-a), (6).

[54] Regulation 2019/947, ANNEX UAS.SPEC.050 (1)a (iv).

[55] For the Privacy by Design principles for UAS suggested by scholars *see* Cavoukian, *Privacy and Drones* [71].

[56] Regulation 2019/947, art 18.

[57] Regulation 2019/947, rec 4.

[58] Regulation 2019/947, art 4–6.

to ensure a Single European Sky [84].[59] If assumed that a Member State opts in for the applicability of these rules to their state aircraft, law enforcement UAS operations, depending on their specific purposes, could fall under 'open' or 'specific,' categories. Nevertheless, these categories and respective requirements will be examined solely from a privacy perspective.

i. *'Open' category of UAS operations*[60]

These UAS operations pose low risk. They maintain a safe distance from individuals, avoid flying over assemblies, and operate within visual line of sight (VLOS) with a maximum altitude of 120 m. They also do not carry hazardous materials or engage in material-dropping activities.[61]

Law enforcement operations under the '*open*' category include monitoring pollution and environmental hazards, assessing biological and chemical risks, and conducting mapping and earth observations for regulatory enforcement and civil protection" purposes. These operations may involve flights over people but take place outside urban and populated areas.

For certain sub-categories of '*open*' UAS operations, the remote pilot (e.g., law enforcement officer) must complete an online training course and theoretical knowledge examination.[62] Notably, the examination includes testing the pilot's knowledge of privacy and data protection [79]. While the privacy results are not the sole factor in the overall test outcome, it represents a commendable step towards bolstering privacy and data protection awareness among exam participants.

ii. *'Specific' category of UAS operations:*

LEAs' UAS operations, especially in urban settings, frequently involve flights over people or assemblies. These operations, not meeting the open category's criteria, result in higher privacy and data protection risks.

Examples from law enforcement include crowd control operations, UAS disposal of pepper gas [24], and UAS surveillance of public spaces for predictive and preventive policing. Due to the increased risks of specific category operations, LEAs must obtain airworthiness authorisations, operator licenses and adopt "*additional operational limitations or higher capability of the involved equipment and personal*".[63]

To conduct "specific" category operations, LEAs, as the UAS operators, must provide a statement confirming compliance with relevant EU or national-level privacy rules.[64] Additionally, submission of an "operations manual" examining compliance with privacy requirements is mandatory.[65] These requirements, although standard clauses, uphold the data protection principle of accountability.

iii. *'Certified' category of UAS operations:*

These (e.g., air taxis, international cargo drones) pose risks akin to manned aviation.[66] LEAs, to our knowledge, do not operationalise UAS falling under this category.

Despite its traditional focus on safety, aviation law increasingly recognises privacy and data protection risks. Besides, a new approach of "safety beyond physical interaction" is suggested by scholars [85]. Accordingly, with the integration of AI into UAS, safety considerations should encompass multiple dimensions; temporal aspects, cybersecurity measures, interactive elements, and societal implications [85]. This broader concept of safety requires aviation legislation to address also data ownership, privacy, cybersecurity, and psychological impacts of surveillance to establish comprehensive safety standards for UAS-human interactions.

4 Proposal for an Artificial Intelligence Act (AIA)

The Proposed Artificial Intelligence Act (Proposed AIA) [86], together with the proposed amendments [87], outline a list of prohibited practices posing unacceptable risks, significantly important for LEAs' UAS payloads. The list includes biometric identification, predictive policing, emotion recognition systems, and real-time remote biometric identification (with exceptions).[67]

AI use in law enforcement context is also deemed high-risk and is imposed with stricter obligations. The provisions and recitals of the proposed text includes specific references to AI use for law enforcement purposes.[68] Moreover, privacy and data governance is deemed as a general principle whereby all AI systems "*shall be developed and used in compliance with existing privacy and data protection rules,*

[59] 'Single European Sky' is an initiative of the European Union (EU) aimed at creating a unified and harmonized airspace system across Europe.

[60] For requirements for "open" category UAS operations see, Regulation 2019/947, art 4.:

[61] Regulation 2019/947, art 4.

[62] Regulation 2019/947, Annex Part A UAS.OPEN.020 (4-b).

[63] Regulation 2019/947, art 5(1);

[64] Regulation 2019/947, art 12.

[65] The risks and complexity LEAs' high impact UAS operations necessitates the manual, Regulation 2019/947, UAS.SPEC.030 (3)(e).

[66] Regulation 2019/947, art 6.

[67] Proposed AIA, art 5(1- (a)(d)).

[68] Proposed AIA, art 5 (1)(a-d), Annex III (1)(b,d,f,g), rec 38.

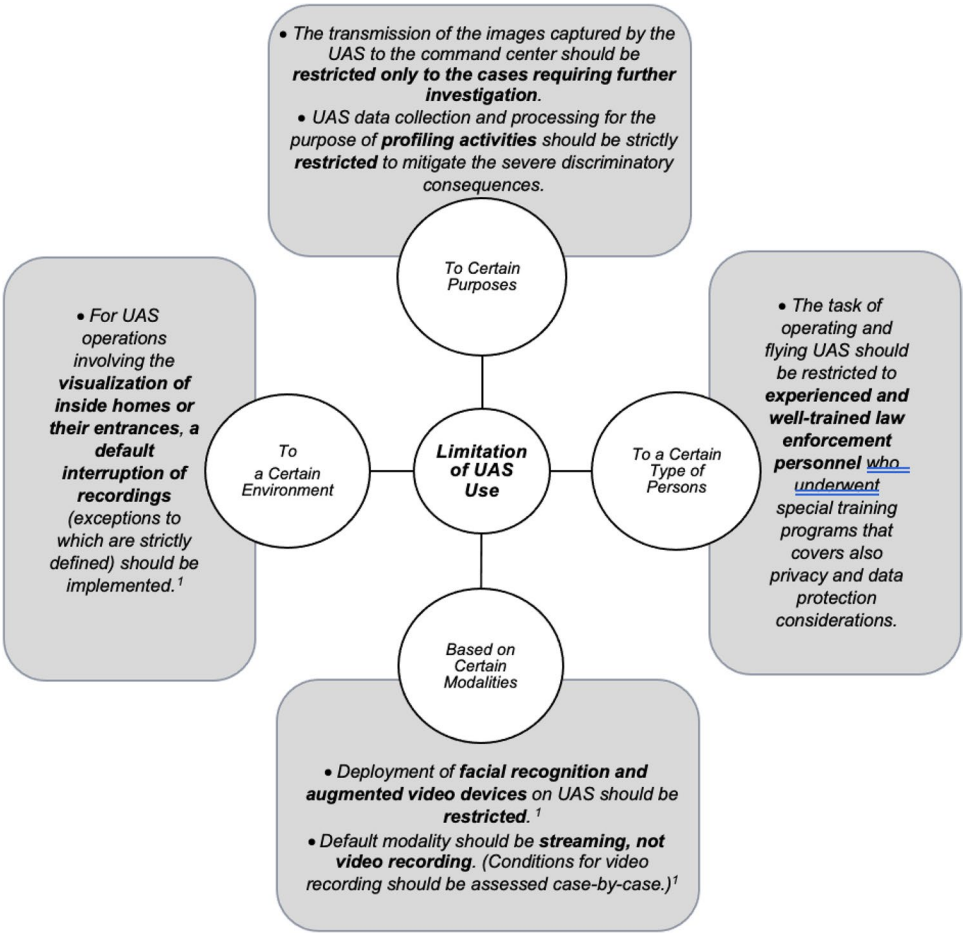

Fig. 2 Additional restrictions on the UAS use

while processing data that meets high standards in terms of quality and integrity".[69]

On the other hand, it should be recognised that the AIA alone cannot be relied upon to address all privacy and data protection risks of UAS and AI payloads for several reasons. Firstly, the AIA's obligations are directed mostly towards providers rather than the users (such as LEAs).[70] Secondly, the prohibition primarily pertains to making these AI tools available, leaving room for the sale of general-purpose AI systems configurable by users [88]. Lastly, the AIA's focus on EU free movement competencies rather than fundamental rights limits its ability to address privacy and data protection concerns comprehensively [88].

[69] Proposed AIA, art 4(a).

[70] Defined by the Proposed AIA as the operator, "the deployer, the authorised representative, the importer and the distributor;" art 3(1–8).

5 Policy Recommendations for Privacy and Data Protection Issues of Law Enforcement Use of UAS

Building upon the regulatory framework analysis in the face of emerging risks, certain steps are necessary to be taken to mitigate the risks against the fundamental rights of the data subjects. These involve various stakeholders including European and National policymakers, Data Protection and Civil Aviation Authorities ("CAA"), the UAS industry, and LEAs.

5.1 Regulatory Suggestions

Notable deficiencies in the current regulatory framework for LEAs' use of UAS are identified. Two different approaches can be taken to address these deficiencies. The first approach involves Member States adopting dedicated domestic legislation that specifically addresses UAS and privacy concerns, considering the unique aspects and challenges faced by LEAs. The second approach entails identifying regulatory gaps and implementing suitable measures, such as amending existing regulations or utilising soft law materials, such as DPA guidelines, EU recommendations, and UAS

Codes of Conduct for LEAs, to address and rectify these gaps effectively.

The dynamic and innovative drone industry, constantly introducing new technologies, payloads, and capabilities, makes the first approach unreasonable to adopt. It goes against the principle of technolical neutrality, involves a time-consuming legislative process, and risks creating outdated laws even before they are enacted. Moreover, regulatory deficiencies arise mainly from enforcement and adaptability, rather than a lack of applicable legislation. Therefore, the second approach, a more agile and adaptable regulatory framework, is better suited to address UAS regulatory gaps and emerging challenges effectively.

5.1.1 Clarifying the Scopes of the GDPR and LED

To tackle the challenge posed by ambiguous terms in the LED, it is recommended to establish clear EU-level definitions. Furthermore, the European Commission's Legal Service's recent recommendation to rely on domestic definitions of "criminal offence" should be reviewed. This would address the fragmented landscape among Member States and ensure equal protection for EU citizens for UAS operations under the LED.

5.1.2 Discretion Afforded to Member States

The tension between EU harmonisation and national sovereignty arises also regarding the LED's application to UAS operations. However, broad derogations within the LED, (e.g., domestic laws allowing decisions based solely on automated processing) may result in Member States employing invasive profiling tools, undermining the core objectives behind the right to privacy and data protection. Hence, while recognising the need for flexibility in regulating the law enforcement sector, which concerns national affairs, the EU's fundamental objectives, including a high level of fundamental rights protection, should be kept in mind. To strike such a balance and realise the intended level of protection envisioned by the LED for UAS operations, a comprehensive review and precise translation of the LED into national laws is necessary.

5.1.3 The Necessity of Additional Restrictions

Usage restrictions are potential tools to safeguard UAS applications by limiting their use to specific individuals, purposes, environments, or modalities [14]. These restrictions can be imposed through regulations, directives, or codes of conduct. Drawing from observed best practices, recommended examples of usage restrictions enhancing privacy and compliance are outlined in the Fig. 2.

Accommodating the diverse operational requirements of LEAs may make it challenging to create an exhaustive list of restrictions and their respective exceptions for UAS. Consequently, the EU should establish dedicated regulatory tools providing technical and detailed provisions, such as regularly reviewed Code of Conducts tailored for UAS use of LEAs, to ensure consistent application of usage restrictions. Some member states already implemented usage restrictions for LEA's UAS (complemented by National Data Protection Authorities (DPAs))' guidance. However, EU-level harmonisation on usage restrictions can significantly minimise LEAs' interference to privacy and data protection.

5.1.4 Recommendations on the regulation of UAS AI tools

The GDPR and LED enforcement deficiencies on automated decision-making can be addressed if their harmonised application with AIA mechanisms can be achieved. Data protection and privacy considerations can effectively be enforced into payload designs through conformity assessments and post-market monitoring outlined in the AIA.[71] Thus, it is recommended to incorporate these considerations into de facto binding [90] technical standardisation processes [91].[72] Nevertheless, total reliance on the AIA for prohibiting invasive AI applications is misleading. Ensuring the safeguarding of UAS data collection and processing, which serves as the fundamental input for invasive profiling and predictive policing activities, must be a paramount priority.

In addition to the prohibition imposed by the AIA on "providers", it is recommended that member states also enact restrictions directed toward LEAs on the use of AI UAS payloads categorised as "unacceptable risk". For the remaining AI UAS payloads, periodic development of specific guidance materials tailored for the UAS use of AI tools by the LEAs is necessary.

5.1.5 Democratic Controls

One of the regulatory gaps lies in outdated national surveillance regimes that do not address the risks posed by advanced surveillance tools such as drones. A certain level of democratic control is sustained through the independent Supervisory Authorities (also known as Data Protection Authorities).[73] However, these controls remain insufficient as UAS as a nocel technology circumvent traditional democratic checks and balances, raising concerns for privacy and

[71] *See* Mökander J and others, 'Conformity Assessments and Post-Market Monitoring [89].

[72] AIA, art 40.

[73] LED, art 41.

accountability. Four suggestions are put in place to sustain democratic control over UAS operations.

i. Decisions regarding the deployment and policies of UAS should be democratically determined through transparent processes, rather than being solely based on funding or department policies within LEAs [71].
ii. UAS investment process should include an independent auditing mechanism to monitor LEAs' UAS usage. This auditing process would offer citizens and watchdog organisations essential information regarding the frequency and nature of UAS surveillance, the effectiveness of initial deployment objectives, public expenditure value, and any functional expansions[71].
iii. UAS operations should be subject to judicial authorisation before the flight. Some instances of warrant requirements can be observed within the EU [14]. Contrarily, some scholars oppose a blanket warrant requirement for all UAS operations, as it over-regulates risks [92]. Indeed, certain UAS operations, such as public space surveillance or search and rescue missions in remote areas, may not require a warrant [93]. However, a general warrant requirement harmonised at the EU level should be established for UAS constituting search (e.g., the use of thermal or high-resolution cameras within residential areas) [14], with well-defined exceptions for emergencies such as hostage scenarios.
iv. Member states should appoint effective independent supervision after the UAS surveillance measure. This would allow for monitoring the effectiveness and impacts of UAS operations, such as function creep or dehumanisation of surveillance. DPAs and Surveillance Oversight Bodies can be appointed as supervisory bodies. Considering the workload and resource limitations of general DPAs, it is recommended to establish a dedicated DPA body focused on regulating and monitoring data collection and processing by LEAs.

5.1.6 Normalisation of the Exceptional Rulemaking

Although UAS deployment by LEAs in the EU predates the COVID-19 crisis, their utilisation during the pandemic's exceptional circumstances was significant. UAS regulatory provisions, enacted under emergency powers, persisted beyond the resolution of the pandemic. The new decree legalising LEAs' use of "airborne cameras" in France [94] can be shown as an example of how UAS legal and political processes went under a process of normalisation of exceptionalism [58]. However, the transition from exceptional UAS rules to normal circumstances requires prudent implementation, ensuring essential safeguards for privacy and data protection. Hence, it is advisable to clarify the ambiguous boundary between exceptional and regular UAS rules to sustain the primacy of fundamental rights and public consultation and bring along short-cut public acceptance processes (e.g., dialogues, and awareness raising) [58].

5.2 The Enforcement of the Existing Legal Framework

Enforcement of the applicable UAS privacy rules poses the primary challenge in balancing the right to privacy and data protection with LEAs' beneficial use [14]. Recommendations for enhanced enforcement of data protection principles are as follows:

- **Storage limitation** (under the LED framework)[74]: Recommendations of the WP29, on adjusting different storage periods for different types of crimes and adopting automatic deletion and anonymisation measures after maximum retention periods, should be implemented by national LEAs [46]. Incorporating EU-wide harmonised retention periods into LED, would significantly strengthen enforcement and amplify the protection afforded by the storage limitation principle.
- **Geographical zones:** Its enforcement should be supplemented by geo-fencing tools to effectively limit UAS access to areas with heightened privacy risks.[75] The competent authorities establishing these geographical zones[76] should possess the requisite expertise in data protection, either through collaboration with DPAs or through specialised training.
- **Necessity and Proportionality Test:** To assess the proportionality and necessity of UAS use and explore less intrusive alternatives for each deployment purpose, internal mechanisms should be established by LEAs (e.g., checklists, authorisation processes). These mechanisms should be supported by the expertise of the DPAs and empirical research assessing the actual effectiveness of UAS operations for each purpose of deployment.
- **Third-country personal data transfers:** Despite formal safeguards, the lack of adequacy decisions for the LED and inadequate enforcement hampers the desired level of protection. To promote EU data protection standards, LEAs should prioritise UAS models from manufacturers storing data within the EU or providing local data collection options.[77]This proactive approach can influence the UAS market and incentivise manufacturers to align with

[74] LED, art 5.
[75] Regulation 2019/947, art 18.
[76] Regulation 2019/947, art 18.
[77] *See* for instance, *DJI – Introducing DJI Government Edition* [95].

EU regulations. For instance, AVY, an EU-based drone manufacturer, actively complies with data protection and EASA rules even for its state aircraft designs [96].

- **Purpose specification and limitation:** Member states must mandate LEAs to establish procedures for operational documentation before the specific UAS use. These documentations must describe UAS operations' purposes with precise and comprehensive detail. Any unauthorised deviation from these purposes, resulting in the collection and use of data for alternative purposes, should render the UAS-collected data and inferred data inadmissible in court proceedings, following the "fruit of the poisonous tree" doctrine [97].

5.3 Technical Solutions

These mitigation measures are found on two levels, technical measures integrated into the UAS software or hardware components and organisational measures implementing rules for operationalising or limiting certain applications [70]. Nonetheless, it is important to note that these suggestions are based only on the current landscape of UAS operations, and the technology and law enforcement use cases evolve rapidly.

5.3.1 Data Protection Impact Assessment

Addressing the distinct risks associated with various UAS payloads and evolving technical capabilities requires conducting DPIAs continuously and adaptively [46]. This involves revisiting certain aspects multiple times, conducting separate analyses for different payloads, and periodically repeating the process as needed. Publicising conducted DPIAs can address the lack of transparency and fairness by informing individuals about UAS data processing activities. This promotes public acceptance and reduces dystopian perceptions surrounding LEAs' UAS use, due to demonstrated compliance with data protection regulations [70].

DPIAs[78] and specific operational risk assessment (SORA) (under aviation regulations)[79] should be integrated to complement each other's functions. In this regard, National DPAs should coordinate their work with National CAAs [98]. Establishing a clear framework for the relationship between the two assessments can address privacy and safety risks together and most effectively.

Combining DPIAs with the authorisation process for operations under the "specific" category would set CAAs as the natural gatekeepers of UAS activity before LEAs are authorised to fly. Nevertheless, CAAs have limited data protection expertise. Thus, their gatekeeper role should be confined to verifying DPIA completion and referring specific cases to DPAs for further guidance and assessment [14]. This coordinated effort, leveraging the expertise of both authorities, can enhance the much-needed enforcement of privacy considerations in practice.

To improve the efficacy of DPIAs, DPAs (both at the EU and Member State levels) should produce comprehensive DPIA guidelines tailored for LEAs. While several DPAs have issued DPIA guidance in the GDPR context, they are not law enforcement-specific. Currently, there are no established EU-wide guidelines, methodologies, or frameworks for conducting DPIAs under the LED [70]. Notably, the "UK guidelines on law enforcement processing" offer valuable specific, and comprehensive guidance for the law enforcement sector [99].

5.3.2 Privacy by Design

A challenge in applying the PbD approach is the absence of a clear definition and standardised framework for translating it into engineering practices [100]. Cavoukian, the developer of PbD concept, has provided specific insights on implementing PbD in UAS [71]. The list below briefly describes Cavoikan's 7 key PbD principles for UAS and provides examples for law enforcement [71].

1)Proactive not Reactive, Preventative not Remedial: LEAs must implement proactive technical and organisational measures before the harm is materialized such as;

- Limitations on the geographical area of operation,
- Limitations on the authorisation of payloads and personnel.

2)Privacy precautions as the Default Setting: UAS used by LEAs should be designed to prioritise privacy by default, even in the absence of user action. These design choices include;

- UAS cameras with limited angles to minimise unintended data collection in privacy sensitive environments,
- Restricted autonomy for field officers in adjusting camera settings such as zooming and manipulating the camera view,
- Default state of UAS audio-visual data collection set to "off."

[78] Besides being a requirement under the LED and GDPR, conducting DPIAs is also required by Regulation 2019/947 for "specific" category operations; Regulation 2019/947, ANNEX UAS.SPEC.050 1(a-iv).

[79] Regulation 2019/947, art 11.

- Activation of infrared sensors and other remote sensing equipment only when necessary.

3)Privacy Safeguards Embedded into UAS Design: An iterative process is needed until privacy becomes "an essential component of the core functionality being delivered." Examples of key measures contributing to this overarching goal include;

- Adoption of privacy-friendly payloads on UAS.
- Utilisation of conventional face-blurring methods and innovative anonymising tools such as tools transforming of identified faces in videos into different faces,
- Use of anonymous video analytic tools that instantly destroy frames in real-time upon detecting identifiable information,
- Automatic shutdown of data collection when UAS strays and deviates from designated area,
- Automatic erasure of data following flights in LEAs' UAS operations not requiring data retention (e.g., crowd monitoring) to minimise the amount of stored data,
- Deployment of cryptographic techniques at the organisational level to safeguard personal data against unauthorised access. (Using encryption methods, personal data can be secured, and encrypted objects can only be unlocked with a secret key),
- Use of strong encryption tools for keeping visual or biometric data collected by UAS and the additional information required to identify individuals separately,
- Secure storage and authorised access for detained UAS data to decrease the risk of their combination.

)Embedding privacy safeguards should allow full functionality: Instead of a heavy compromise between public security and privacy, both the legitimate interests of the LEAs and privacy concerns must be satisfied. For example by;

- Proactively ensuring the secure storage and authorised access for detained UAS data if the detention of certain UAS data is necessary for criminal investigations,
- Using sufficient physical and digital encryption and logs to track instances of access.

5)End-to-end security: A full lifecycle of personal data protection should be ensured by;

- Conducting Data Protection Impact Assessments (DPIAs) TO ensure monitoring a complete lifecycle of compliance with data protection principles and allow LEAs to make informed UAS policy decisions

6)Visibility and Transparency: Keep it Open: LEAs' UAS operations must be visible and transparent to all stakeholders, including the public. This involves;

- Exceeding the informational requirements under the GDPR and LED, for UAS with algorithmic or AI tools.
- Establishing common platforms for public consultation on UAS operations to foster an environment of openness and inclusiveness.

7)Respect for User Privacy: Keep it user-centric: The focus of the design of the LEAs' UAS should remain on empowering individuals in their privacy choices by;

- Implementation of strong privacy defaults,
- Provision of appropriate notice.

To overcome challenges related to the visible invisibility of UAS, it is recommended to make LEAs' UAS more conspicuous through design elements that enhance noticeability [107]. This can include incorporating features like blue and red lights clearly indicating the data controller's identity and audio or visual signalling mechanisms to alert individuals when data collection is active. While examples of such applications exist, harmonising LEAs UAS design within the EU could establish a shared understanding for identifying law enforcement UAS, akin to the universal use of blue and red lights for police forces.

Lastly, considering the difficulty of a clear translation of PbD into engineering practices and the limited technical expertise of LEAs, competent authorities should provide specific guidance for PbD implementation LEAs use of UAS. This guidance should offer practical examples and suggestions for state-of-the-art technical measures, building upon Cavoukian's principles. It should be regularly reviewed and updated to align with the latest advancements in attachable payload capabilities.

5.3.3 Access Controls

It is recommended to incorporate access controls into LEAs organisational processes to manage UAS data collection and processing effectively, limit it to what is necessary for specific, lawful goals and prevent its potential misuse.

Access controls can take various forms [108]. For instance, physical barriers should be utilised in privacy-sensitive contexts, such as for control rooms overseeing beyond visual line of sight (BVLOS) UAS operations or algorithmic UAS data applications. These include video surveillance and modern security methods such as key cards or biometric authentication [109]. Similarly, logical access controls within the software offer valuable adaptability to

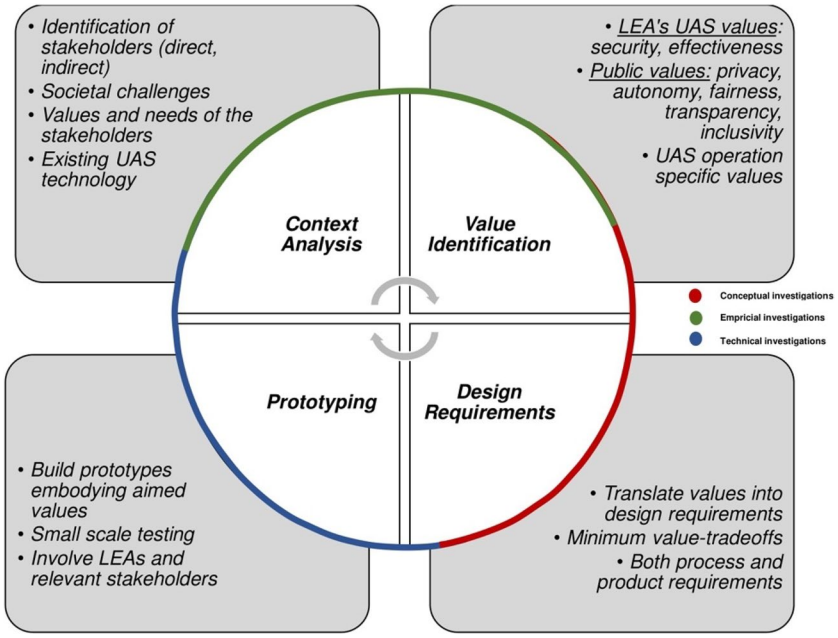

Fig.3 Value Sensitive Design in the Context of Law Enforcement

specific UAS operations and embodied risks, as they can be discretionary, mandatory, or role-based [110].

Combining access controls with other tools and protocols enhances safeguards further. Firstly, their combination with anonymisation and pseudonymisation tools allows privacy-preserving but also efficient use of UAS data [70]. For instance, UAS data, after the identifiable data is removed, can be made visible to personnel within the LEAs at large. Still, authorised personnel whose specific assignments necessitate exclusive access to detailed information about data subjects can view full UAS data during data storage periods. Secondly, incorporating logging and recordkeeping protocols into access controls allows traceability of misuse of UAS data, and contributes to the principle of accountability [70].

5.3.4 Value Sensitive Design

For all designers within the UAS chain, including the payload manufacturers, addressing privacy and data protection is a multifaceted process. It requires also acknowledging the indirect consequences of the mishandling of personal data, such as discrimination and function creep, achievable through Value Sensitive Design.[80] VSD, comprised of conceptual, empirical, and technical investigations, shares notable similarities with PbD [112]. However, while prioritising human values throughout the technical design process, VSD encompasses more than privacy concerns, as elaborated in the Fig. 3.

Integrating VSD into the design of UAS, its payloads, and algorithmic tools contribute to fairness, algorithmic accountability, and intelligibility of LEAs' data collection and processing activities. VSD addresses privacy and data protection holistically, undertaking both direct and indirect consequences within the value tensions underlying LEAs' UAS use.

5.3.5 Human in the Loop

Although the current UAS used by LEAs involves AI payloads only for algorithmic analysis, rather than full automation, future possibilities are not limited by existing legislation. Moreover, the UAS landscape for law enforcement is complex, with imbalanced power dynamics and diverse vulnerabilities. Present AI technologies lack full comprehension of this context and require human oversight to ensure ethical and trustworthy systems [113].

GDPR and LED protect individuals against fully automated decisions,[81] assuming any human involvement is a sufficient safeguard. However, for effective protection, human oversight must be "*meaningful*" [47]. The interaction between supervisory humans and the UAS automated decision-making mechanisms faces two key problems: complacency risks and automation bias [114]. Firstly, law enforcement personnel assigned to monitor UAS operations often have a passive role, risking delayed reactions and increased negligence (assuming the personnel is not the remote pilot) [115]. Secondly, humans interacting with UAS automated

[80] *See for instance,* DJI Enterprise Drones, [111].

[81] LED, art 11; GDPR, art 22.

processes may exhibit automation bias, attributing excessive authority, credibility, infallibility, and superiority over human judgment [114].

Consequently, to ensure "meaningful" human oversight, law enforcement officers should receive comprehensive training on UAS decision-making algorithms' functions and fallibility. To mitigate complacency, human oversight duties should go beyond passive observation of UAS visuals and audio and require active involvement.

5.4 Stakeholder Cooperation

The UAS stakeholder landscape in law enforcement is complex, consisting of public, complex supply chains and actors with varying backgrounds in legal, technical, aviation and privacy domains. Only through strong cooperation can these stakeholders complement each other's policies and inadequacies and implement the above-described recommendations. Consequently, this article proposes certain policies and actions to the stakeholders involved in LEAs UAS operations. Nonetheless, it should be noted even though the below recommendations are categorized under individual stakeholders for convenience reasons, they are interlinked with other recommendations and require close cooperation of other stakeholders.

i. Law Enforcement Authorities

LEAs should raise awareness among their officers and UAS operators regarding data protection and privacy [14]. Developing training courses and high-quality information as well as a cross-national resource similar to current flight tracking systems,[82] specifically dedicated to LEA's UAS operations (excluding covert surveillance) can greatly enhance transparency, fairness and accountability and requires cooperation with the CAAs.

In terms of field operations, if sharing UAS surveillance information jeopardises the mission's effectiveness, data subjects should be notified at least after the UAS surveillance within a reasonable timeframe for enhanced transparency [117].

ii. Data Protection Authorities

Data protection rules are complex and deliberately broad in scope to ensure technological neutrality. Law enforcement officers operating UAS or payload and UAS manufacturers may lack legal in legal data protection. Thus, intelligible guidance beyond legal jargon for the GDPR and LED framework, UAS code of conduct, and law enforcement-specific DPIA templates should be developed by both EU-wide and national data protection bodies [14]. The United Kingdom (UK) Information Commissioner's Office (ICO)'s guidelines serve as a commendable example [99].

Besides the LEAs and manufacturers, DPAs should actively inform also the public and run awareness raisin campaigns of UAS data collection and processing activities by LEAs, empowering them to exercise their rights effectively.

iii. Aviation Authorities

Aviation Authorities should actively promote integrating privacy and data protection into the safety framework, emphasising their interlink. Recommended examples include a stronger emphasis on privacy requirements within the existing authorisation processes and operator training and coordinating SORA 2.5 and DPIAs effectively to de facto establish CAAs as data protection gatekeepers. Due to payloads being the primary source of privacy risks [77], the option to develop a separate authorisation process for attachable payloads should be explored.

Aviation Standardisation Authorities in the EU, such as the European Organization for Civil Aviation Equipment, should incorporate privacy considerations into technical standards to enhance privacy and data protection rights. These standards can play a pivotal role in elevating data protection remedies by integrating privacy into the compliance considerations of manufacturing companies.

iv. UAS Manufacturers

UAS manufacturing involves complex supply chains. Not only drone manufacturers but also payload manufacturers should actively prioritise data protection [14] and incorporate VSD and PbD approaches into their designs while recognising the specific requirements and sensitivities associated with UAS applications in law enforcement.

Manufacturers must recognise the specific requirements and sensitivities associated with UAS applications in law enforcement. Accordingly, they should create customised versions of their products specifically designed for law enforcement purposes, demonstrating their maximum commitment to upholding data protection. With the active support of the European Commission and national policymakers, the UAS industry and its associations should forge strong partnerships with DPAs to devise shared risk mitigation strategies for law enforcement operations and to stay up-to-date about privacy-preserving technologies.

v. The European Commission

[82] *See for instance* system, Flightradar 24, [116].

The European Commission should establish a stakeholder forum for interactive discussions between relevant experts, stakeholders and LEAs regarding UAS operations [14]. Various options such as workshops, seminars, an online portal and working groups [14], should be explored to ensure progress and resolution of UAS issues in law enforcement.

vi. Member States

To uphold civil aviation standards in law enforcement operations, it is recommended for Member States to opt-in for the application of EASA rules to their state aircraft, albeit with limitations. While the application of these rules to military UAS operations may have adverse consequences, their implementation in law enforcement aircraft, such as police drones, can significantly contribute to safeguarding individuals' rights to privacy and data protection [14].

vii. Public

Previously, public distrust has led some municipalities to impose outright bans on drone usage by LEAs [118], highlighting the need to address privacy and data protection concerns to foster public acceptance of UAS in law enforcement [119, 120]. Enhanced public involvement is central to the transparency and accountability of LEAs' UAS operations. Efforts should be made to educate the public on UAS data collection activities and respective rights through mediums such as billboards, signposts, information sheets, dedicated sections on LEA websites, social media platforms, and targeted awareness campaigns [14].

Nonetheless, the public input should remain meaningful. Feedback and input particularly from marginalised communities (often disproportionately impacted by LEA's UAS activities) should be obtained. This is crucial for fair and inclusive decision-making in LEAs' UAS operations.

6 Conclusion

While LEAs are still far from deploying UAS as a means of 24/7 surveillance, these aerial technologies are increasingly infiltrating the realm of surveillance, gradually supplanting conventional law enforcement methods for various purposes. This increasing utilisation of UAS by LEAs occurs within a dynamic and intricate environment characterised by value tensions among diverse stakeholders with varying backgrounds. Among these value tensions, the right to privacy and data protection emerges as a critical bottleneck to restraining the exercise of state power and mitigating the risk of surveillance societies from taking root.

In the face of these risks posed, the adequacy of the EU legal framework in safeguarding the right to privacy and data protection against the UAS use of the LEAs is largely dependent on the circumstances and the purposes behind specific UAS operations. It extends beyond mere applicability discussions and requires understanding the risks associated with specific use cases and a closer examination of various factors, such as an ever-increasing variety of payloads, integration of AI into UAS, and UAS involvement in surveillance data assemblies.

Nonetheless, the privacy and data protection safeguards for UAS use cases posing medium to high-level risks remain inadequate. Structural safeguards, data protection principles, and subject rights are provided within privacy legislation. However, the ambiguity of GDPR and LED's material scope hinders a clear understanding of structural safeguards, rights, and obligations for both data subjects and LEAs. This results in arbitrary applications of the LED, affording rather limited protection to data subjects. Besides, the data protection principles outlined in the privacy legislation are often problematic within UAS use due to the technical limitations, nature of UAS data collection, and LEAs' limited expertise in privacy concerns.

The current aviation framework, although not applicable to LEAs' aircraft unless member states opt-in, promotes identifiability, transparency, and accountability. It can complement the generic privacy safeguards with its effective enforcement mechanisms. While the aviation sector's growing interest in privacy and data protection as a secondary matter is notable, greater commitment is necessary to co-enforce privacy and aviation regulations. Discussions persist about whether aviation authorities, like EASA, possess the competence to regulate matters indirectly related to safety, and the intricate interplay between data protection and safety in this context. Lastly, the AIA regulates UAS operations concerning AI payloads. However, its contribution is limited to addressing risks, fairness and transparency in the UAS market as AIA's personal scope pertains to providers and does not impose obligations on LEAs.

To address this insufficient enforcement, collaboration among UAS stakeholders is necessary to develop high-quality soft law, including data protection guidance materials and UAS codes of conduct, and ensure their effective implementation. Nevertheless, these materials' legally non-binding nature deems stakeholder commitment to data protection privacy essential.

LEAs navigate a complex path where finding a balance between scalability and sustainability is required to enable the ethical use of UAS and the development of sustainable urban air mobility. Deploying technical tools in line with Lessig's concept of "code" can significantly reduce adverse impacts. By implementing organisational, hardware, and software solutions that eliminate privacy-invasive options, UAS itself can enforce compliance. On the other hand, it is important to exercise caution and avoid falling into the

common dilemma of techno-solutionism. Relying solely on technology as the solution to all complex privacy and data protection concerns, without considering broader societal and ethical implications, should be refrained from. Instead, a comprehensive approach comprising the interplay between privacy and aviation laws, societal expectations, and democratic controls is needed. Only by doing so, LEAs'.

UAS use can best benefit society while simultaneously safeguarding the protection of privacy and data rights.

Acknowledgements Special thanks to *Dr. Benjamyn Scott* for his invaluable feedback and guidance throughout the development of this article. This work was initially written as a master's thesis and has been revised to meet the requirements of publication in a peer-reviewed journal.

Author's Contributions The following authors contributed equally to all aspects of the study.

Funding The author declares that no funds, grants, or other support were received during the preparation of this manuscript.

Data Availability Not applicable.

Declarations

Conflicts of Interest The author has relevant financial or non-financial interests to disclose.

Ethics Approval Not applicable. No animals, including humans, were studied in any way during the writing of this paper.

Consent to Participate This study did not involve any 3rd party participation. All authors consent to participation.

Consent for Publication This study did not involve any 3rd party participation. All authors consent to publication.

References

1. Scott, B.I., (ed).: The Law of Unmanned Aircraft Systems (Second edition, Wolters Kluwer Law International, B V 2022)
2. Wagen, W., van der, Oerlemans, J-J.,Weulen Kranenbarg, M. (eds).: Essentials in Cybercrime: A Criminological Overview for Education and Practice (Eleven 2022)
3. Ministerie van Justitie en Veiligheid.: Police Powers - Police - Government.Nl' (22 March 2013) <https://www.government.nl/topics/police/police-powers> accessed 14 March 2023
4. About CBP | U.S. Customs and Border Protection' <https://www.cbp.gov/about> accessed 14 March 2023
5. (*About us - Sistema di informazione per la sicurezza della Repubblica*) <https://www.sicurezzanazionale.gov.it/sisr.nsf/english/about-us.html> accessed 14 March 2022
6. Guild, E., (ed).: The Area of Freedom, Security and Justice Ten Years on: Successes and Future Challenges under the Stockholm Programme (Centre for European Policy Studies 2010)
7. 'Law Enforcement' (*DJI*) <https://enterprise.dji.com/public-safety/law-enforcement> accessed 9 July 2023
8. HYBRiX.20, 'Hybrix Long-Endurance Drone – Quaternium' <https://www.quaternium.com/uav/hybrix-drone/> accessed 16 March 2023
9. Jouav CW-40D, 'CW-40 Hybrid Gasoline & Battery Long Endurance Drone' (*JOUAV*, 19 July 2022) <https://www.jouav.com/products/cw-40.html> accessed 16 March 2023
10. 'Best Law Enforcement Drones of 2022 | DSLRPros' <https://www.dslrpros.com/dslrpros-blog/best-law-enforcement-drones-of-2022/> accessed 2 November 2023
11. Klauser, F,: Police Drones and the Air: Towards a Volumetric Geopolitics of Security 27 Swiss Political Science Review 158 (2021)
12. Barrows, R.S.: Drones and Law Enforcement in AA Tarr and others (eds), Drone law and policy: global development, risks, regulation and insurance (Routledge Taylor & Francis Group 2022), 58
13. Hodgkinson, D., Johnston, R.: Aviation Law and Drones: Unmanned Aircraft and the Future of Aviation (Routledge 2018)
14. European Commission Directorate General for Enterprise and Industry ("DG-ENTR"), Trilateral Research & Consulting, and Vrije Universiteit Brussel, Study on Privacy, Data Protection and Ethical Risks in Civil Remotely Piloted Aircraft: Summary for Industry (Publications Office 2014)
15. Dodd, V.: Drones Used by Police to Monitor Political Protests in England The Guardian (14 February 2021) <https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion> accessed 14 March 2023
16. (Riot Control Drone System - ISPRA LTD) <https://www.ispraltd.com/Riot-Control-Drone-System.html>
17. Wray, S.: Barcelona Uses Drones to Monitor Beaches (Cities Today, 23 June 2022) <https://cities-today.com/barcelona-uses-drones-to-monitor-beaches/> accessed 14 March 2023
18. 'Sporadic Violence in France for Fifth Night of Rioting as Police Tear Gas Protesters in Marseille, with Drones Deployed in Paris Suburbs - ABC News' <https://www.abc.net.au/news/2023-07-02/france-riots-nahel-protests/102551792> accessed 9 July 2023
19. Pidd, H., Dodd, V.: UK Police Use Drones and Roadblocks to Enforce Lockdown The Guardian (26 March 2020) <https://www.theguardian.com/world/2020/mar/26/uk-police-use-drones-and-roadblocks-to-enforce-lockdown> accessed 14 March 2023
20. King, A.: Sherlock Drones - Automated Investigators Tackle Toxic Crime Scenes | Research and Innovation (*European Commission*) <https://ec.europa.eu/research-and-innovation/en/horizon-magazine/sherlock-drones-automated-investigators-tackle-toxic-crime-scenes> accessed 14 March 2023.
21. Hell, P.M., Varga, P.J.: Assisting Law Enforcement Tasks with Thermal Camera Drones, 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE) (IEEE 2020)
22. Raturi, G., others.: ADoCW: An Automated Method for Detection of Concealed Weapon, 2019 Fifth International Conference on Image Information Processing (ICIIP) (IEEE 2019)
23. 'Mavic 2 Enterprise Advanced - Dual Imaging, Reimagined' (*DJI*) <https://www.dji.com/nl/photo> accessed 14 March 2023

24. Nast, C.: Pepper-Spraying Drones Will Be Used on Indian Protesters Wired UK <https://www.wired.co.uk/article/pepper-spraying-drones> accessed 15 March 2023
25. Autel EVO II Dual, 'Public Safety - Autel Robotics' (*Autel Robotics*) <https://auteldrones.ae/public-safety/> accessed 14 March 2023
26. Lilly, A.: IMSI Catchers: Hacking Mobile Communications 2017 Network Security 5, 7 (2017)
27. Shanthi, K.G, others.: Smart Drone with Real Time Face Recognition 80 Materials Today: Proceedings 321 (2023)
28. Shreedevi, P., Mohana, H.S.: Video Analysis to Recognize Unusual Crowd Behavior for Surveillance Systems: A Review in Sandeep Kumar and others (eds), Third Congress on Intelligent Systems (Springer Nature Singapore 2023)
29. Article 29 Data Protection Working Party (WP29) Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones [2015]
30. Wright, D., others.: Sorting out Smart Surveillance 26 Computer Law & Security Review 343 (2010)
31. Kraus, M. others.: Toward Mass Video Data Analysis: Interactive and Immersive 4D Scene Reconstruction 20 Sensors 5426 (2020)
32. Choi, C.: Theft! Drones Help Fight A Growing On-Site Problem (Inside Unmanned Systems, 19 August 2021) <https://insideunmannedsystems.com/theft-drones-help-fight-a-growing-on-site-problem/> accessed 11 June 2023
33. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") [2016] OJ L119
34. Noack, R.: In Victory for Privacy Activists, France Is Banned from Using Drones to Enforce Coronavirus Rules Washington Post (14 January 2021) <https://www.washingtonpost.com/world/in-victory-for-privacy-activists-france-is-banned-from-using-drones-to-enforce-covid-rules/2021/01/14/b384eb40-5658-11eb-acc5-92d2819a1ccb_story.html> accessed 26 June 2023
35. Burgoon, J.K.: Privacy and Communication 6 Annals of the International Communication Association 206 (1982)
36. Autoriteit Persoonsgegevens, 'Cameratoezicht: Beleidsregels Voor de Toepassing van Bepalingen Uit de Wet Bescherming Ersoonsgegevens En de Wet Politiegegevens' BWBR0037591
37. Directive (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, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) ("LED") [2016] OJ L 119
38. Leiser, M.R., Custers, B.H.M.: The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680 [2019] European Data Protection Law Review
39. Commission Expert Group, Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (7 November 2016)
40. Sajfert, J., Quintel, T.: Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities in Mark Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing Ltd 2017)
41. BrewczyäÑska, M.: A Critical Reflection on the Material Scope of the Application of the Law Enforcement Directive and Its Boundaries with the General Data Protection Regulation' in Eleni Kosta, Ronald Leenes and Irene Kamara (eds), Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022) <https://www.elgaronline.com/view/edcoll/9781800371675/9781800371675.00013.xml> accessed 3 June 2023
42. 'New Dutch Drone Can Find Hidden Graves and Buried Bodies | NL Times' <https://nltimes.nl/2023/05/14/new-dutch-drone-can-find-hidden-graves-buried-bodies> accessed 3 June 2023
43. 'How the Elite Police STAR Unit Takes down a Gunman and Rescues Hostages' (*CNA*) <https://www.channelnewsasia.com/singapore/police-spf-star-unit-special-tactics-rescue-gunman-hostage-3442371> accessed 3 June 2023
44. Welsh, B.C., Farrington, D.P.: Crime Prevention and Public Policy, The Oxford Handbook of Crime Prevention (Oxford University Press 2012)
45. "Law Enforcement Directive": What Are We Talking About? | CNIL' <https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about> accessed 5 June 2023
46. WP29, Opinion 2016/680 on some key issues of the Law Enforcement Directive [2017]. <http://ec.europa.eu/newsroom/article29/item-detail .cfm?item_id=610178> accessed 4 June 2023
47. Quintel, T.: Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive 4 Eur. Data Prot. L. Rev. 10 (2018)
48. Wilkinson, D., Ooijevaar, M.*:* Data protection, privacy & big data' in Tarr AA and others (eds), Drone Law and Policy: Global Development, Risks, Regulation and Insurance (Routledge Taylor & Francis Group 2022), 208
49. WP29, 'Response to the Questionnaire: Remotely Piloted Aircraft Systems (RPAS) ' Ref. Ares(2013)3737090 (2013) https://ec.europa.eu/justice/article-29/documentation/otherdocument/files/2013/20131216_reply_to_rpas_questionnaire.pdf
50. Andrejevic, M., others.: Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance (Aleš Završnik ed, Springer 2016)
51. Opinion on a draft decree implementing Articles L. 242–1 [2023] 2023–027', available at: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047471177 (accessed 25 June 2023)
52. Hartmann, K., Giles, K.: UAV Exploitation: A New Domain for Cyber Power, 2016 8th International Conference on Cyber Conflict (CyCon) 209–210 (2016)
53. 'Iraq Rebels "Hack into US Drones"' (17 December 2009) <http://news.bbc.co.uk/2/hi/middle_east/8419147.stm> accessed 10 May 2023
54. Schermer, B.W.: The Limits of Privacy in Automated Profiling and Data Mining 27 Computer Law & Security Review 45 (2011)
55. 'Adequacy Decisions' <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 4 June 2023
56. Drechsler, L.: The Achilles Heel of EU Data Protection in a Law Enforcement Context: International Transfers Under Appropriate Safeguards in the Law Enforcement Directive' [2020] European Public Law: EU eJournal
57. Council of Europe, Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2018) 223, para 55
58. Martins, B.O., Lavallée, C., Silkoset, A.: Drone Use for COVID-19 Related Problems: Techno-solutionism and Its Societal Implications 12 Global Policy 603 (2021)
59. Quinn, P., Malgieri, G.: The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22 German Law Journal 1583
60. Case C-184/20, *OT v. Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601
61. Ellefsen, H.B., others.: Unpacking Preventive Policing: Towards a Holistic Framework 25 International Journal of Police Science & Management 196 (2023)

62. Weynand, L.L.: Public Safety Agencies and UAV Technology: A Review of Uses 1060 Student Publications, 20 (2021)
63. De-la-Torre, M., others.: Partially-Supervised Learning from Facial Trajectories for Face Recognition in Video Surveillance 24 Information Fusion 31 (2015)
64. R DJS and others.: Real Time Violence Detection Framework for Football Stadium Comprising of Big Data Analysis and Deep Learning through Bidirectional LSTM 151 Computer Networks 191 (2019)
65. Nawaratne, R., others.: Spatiotemporal Anomaly Detection Using Deep Learning for Real-Time Video Surveillance 16 IEEE Transactions on Industrial Informatics 393 (2020)
66. Thakur, N., others.: Artificial Intelligence Techniques in Smart Cities Surveillance Using UAVs: A Survey, Machine Intelligence and Data Analytics for Sustainable Future Smart Cities, vol 971 (Springer International Publishing 2021), 335–342
67. Gstrein, O.J.,Bunnik, A., Zwitter, A.: Ethical, Legal and Social Challenges of Predictive Policing 3 Católica Law Review, Direito Penal 77 (2019)
68. Bracken-Roche, C.: Domestic Drones: The Politics of Verticality and the Surveillance Industrial complex 71 Geographica Helvetica 167 (2016)
69. Sakharkar, A.: Fully Autonomous Drone System for Search and Rescue Operations at Sea (*Inceptive Mind*, 12 July 2022) <https://www.inceptivemind.com/fully-autonomous-drone-system-search-rescue-operations-sea/25408/> accessed 18 June 2023
70. Marquenie, T, Quezada-Tavárez, K.: Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing' in Garik Markarian and others (eds), Security technologies and social implications (John Wiley & Sons, Inc 2023) 35
71. Cavoukian, A.: Privacy and Drones: Unmanned Aerial Vehicles (Information and Privacy Commissioner of Ontario, Canada Ontario 2012)
72. Consolidated Version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01
73. Bassi, E.: European Drones Regulation: Today's Legal Challenges, 2019 International Conference on Unmanned Aircraft Systems (ICUAS) (2019)
74. Regulation 2018/1139 of the European Parliament and of the Council of 4 July 2018 on Common Rules in the Field of Civil Aviation and Establishing A European Union Aviation Safety Agency, and amending Regulations [2018] OJ L212 ("Regulation 2018/1139")
75. Masutti, A., Tomasello, F.: International Regulation of Non-Military Drones (Edward Elgar Publishing Limited 2018)
76. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the Rules And Procedures for the Operation of Unmanned Aircraft (Regulation 2019/947) [2019] OJ L 152
77. EASA Opinion 01/2018, Introduction of a Regulatory Framework for the Operation of Unmanned Aircraft Systems in the 'Open' and 'Specific' Categories [2018]
78. EASA, Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947, [2019], issue 1
79. EASA, Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945) (2021)
80. 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 ("Drone Strategy 2.0") [2022]
81. Scott, B, Andritsos, K.: A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' (2023) 48 Air and Space Law 273
82. Konert, A., Dunin, T.: A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 Advances in Science, Technology and Engineering Systems Journal 93
83. Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems (Regulation 2019/945) [2019] OJ L152
84. 'Single European Sky' <https://transport.ec.europa.eu/transport-modes/air/single-european-sky_en> accessed 26 June 2023
85. Martinetti, A., others.: Redefining Safety in Light of Human-Robot Interaction: A Critical Review of Current Standards and Regulations 3 Frontiers in Chemical Engineering 666237 (2021)
86. Proposal For A Regulation, COM/2021/206 Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts [2021] (AIA)
87. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9–0146/2021 – 2021/0106(COD) [2023]
88. Veale, M., Zuiderveen Borgesius, F.: Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach (2021) 22 Computer Law Review International 97
89. Mökander, J., others.: Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation 32 Minds and Machines 241 (2022)
90. Colombo C and Eliantonio M, 'Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?' 24 Maastricht Journal of European and Comparative Law 323 (2017)
91. Floridi, L.: The European Legislation on AI: A Brief Analysis of Its Philosophical Approach 34 Philosophy & Technology 215 (2021)
92. McNeal, G.: Drones and Aerial Surveillance: Considerations for Legislatures' (*Brookings*, 13 November 2014) <https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/> accessed 25 June 2023
93. Watney, M.: Ethical and Legal Aspects Pertaining to Law Enforcement Use of Drones 17 International Conference on Cyber Warfare and Security 358 (2022)
94. Loi n°2022–52 du 24 janvier 2022, J.O. du 25 Janvier, 2022, art 22
95. *DJI – Introducing DJI Government Edition* (Directed by DJI, 2019) <https://www.youtube.com/watch?v=6HZwQ2vt_38> accessed 25 June 2023, 01:20
96. Fabrique, 'Beginner's Guide: EU Drone Regulations Pt. 1 - Avy - Drones for Good' <https://avy.eu/stories/beginners-guide-eu-drone-regulations-pt-1/> accessed 10 July 2023
97. Geyer, F.: Fruit of the Poisonous Tree: Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy (CEPS 2007), 1
98. Bassi, E.: From Here to 2023: Civil Drones Operations and the Setting of New Legal Rules for the European Single Sky 100 Journal of Intelligent & Robotic Systems 493 (2020)
99. UK Information Comissioner's Office, 'Guide to Law Enforcement Processing' <https://ico.org.uk/for-organisations/guide-to-le-processing/>
100. Rubinstein, I.S., Good, N.: Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. New York University School of Law Pulic Law & Legal Theory Research Paper Series, (12), 4–71 (2012)

101. Kim, M.U., Lee, H., Yang, H.J., Ryoo, M.S.: Privacy-preserving robot vision with anonymized faces by extreme low resolution," in Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2019
102. Lee, H., others.: Privacy-Protection Drone Patrol System Based on Face Anonymization <https://arxiv.org/abs/2005.14390> accessed 23 June 2023
103. WP29, Opinion 05/2014, on Anonymisation Techniques [2014]
104. Cavoukian, A.: Anonymous Video Analytics (AVA) Technology and Privacy' [2011] White Paper, Information and Privacy Commisioner, Ontario, Canada (April 2011)
105. Martin, K., Plataniotis, K.N.: Privacy Protected Surveillance Using Secure Visual Object Coding 18 IEEE Transactions on Circuits and Systems for Video Technology 1152 (2008)
106. Cavoukian, A., Stoianov, A.: Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security AND Privacy', [2007] Information and Privacy Commissioner of Ontario
107. 'Privacy by Design Guide: A DroneRules.Eu PRO Resource for Drone Manufacturers' <https://dronerules.eu/assets/files/DRPRO_Privacy_by_Design_Guide_EN.pdf>
108. Ting, D.; Managing Access Control – Combining Physical and Logical Security 19 Card Technology Today 9 (2007)
109. Norman, T.: Foundational Security and Access Control Concepts', Electronic Access Control (Elsevier 2012) <https://linkinghub.elsevier.com/retrieve/pii/B9780123820280000028> accessed 26 June 2023
110. Collins, L.: Access Controls' in John R Vacca (ed), Cyber security and IT infrastructure protection (1st ed, Syngress is an imprint of Elsevier 2014)
111. 'DJI Enterprise Drones Provide Secure and Reliable Solutions for Government. Read about Them and Our Case Studies.' (*DJI Official*) <https://www.dji.com/enterprise/government> accessed 24 June 2023
112. Friedman, B., Hendry, D.G.: Value Sensitive Design: Shaping Technology with Moral Imagination (MIT Press 2019)
113. High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
114. Adensamer, A.,Gsenger, R., Klausner, L.D.: Computer Says N: Algorithmic Decision Support and Organisational Responsibility 7–8 Journal of Responsible Technology 100014 (2021)
115. Bahner, J.E., Hüper, A-D., Manzey, D.H.: Misuse of automated decision aids: Complacency, automation bias and the impact of training experience. International Journal of Human-Computer Interaction, 669 (2008)
116. Flightradar24, 'Live Flight Tracker - Real-Time Flight Tracker Map' (*Flightradar24*) <https://www.flightradar24.com/> accessed 10 July 2023
117. *Roman Zakharov v. Russia*, App no 47143/06, (ECtHR, 4 December 2015) para 234
118. 'Seattle Mayor Grounds Police Drone Program' *Reuters* (8 February 2013) <https://www.reuters.com/article/usa-drones-seattle-idINL1N0B80XX20130208> accessed 26 June 2023
119. EASA, Study on the societal acceptance of Urban Air Mobility in Europe, (2021)
120. Sabino, H., others.: A Systematic Literature Review on the Main Factors for Public Acceptance of Drones (2022) 71 Technology in Society 10209

E. Öykü Kurtpınar is a Ph.D. candidate at Leiden University, conducting multidis-ciplinary research on Law and Innovative Air Mobili-ty at the Institute of Air and Space Law, Private Law, and eLaw on Law and Innovative Air Mobility.