International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Drone-Related Privacy Violations in the UAE: A Doctrinal Analysis of Regulatory Gaps and Reform Imperatives

Dr, Mariam Mohamed Hassan Alhammadi[1], Salem Saeed Mohammed Eisa ALDEREI[2]

[1,2]Ministry of Interior - Police College, Abu Dhabi

Abstract

Drone-Related Privacy Violations in the UAE: A Doctrinal Analysis of Regulatory Gaps and Reform Imperatives has increasingly drawn scholarly attention within global debates on digital governance and emerging surveillance technologies. While privacy protection has been widely examined in relation to data protection and cyber regulation, existing literature has not sufficiently explored how drone-enabled surveillance challenges legal frameworks, particularly within the United Arab Emirates. This study addresses this gap by examining the adequacy of existing UAE laws in addressing drone-related privacy concerns and evaluating the extent of fragmentation between aviation regulation and cybercrime legislation in protecting personal privacy against drone surveillance risks. The study adopts a doctrinal research methodology through the lens of qualitative analysis, supplemented by academic books, peer-reviewed journal articles, and authoritative reports. It focuses on Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes and Federal Decree-Law No. 26 of 2022 Regulating the Civil Use of Drones. All materials were subjected to rigorous thematic analysis guided by surveillance theory. The findings reveal that cybercrime legislation remains technology neutral and insufficiently responsive to drone surveillance, while drone regulation is predominantly safety oriented with limited integration of privacy and data governance principles. A further key finding is the existence of doctrinal fragmentation between both frameworks, resulting in regulatory gaps, legal uncertainty, and weak protection against non-consensual aerial surveillance. The study recommends legal integration, the development of drone-specific privacy standards, and proactive regulatory mechanisms, contributing to information technology law, cyber law, air and space law, while advancing the interdisciplinary domain of law and technology as its departure area.

Keywords: Cybercrime; Drone Operations; Privacy Violation; Surveillance Theory, Unmanned Aerial Vehicles.

1. Introduction

The rapid advancement of unmanned aerial vehicles (UAVs), commonly referred to as drones, has significantly transformed contemporary practices of surveillance, data collection, and aerial monitoring (Mohsan, et al., 2023). As noted by Barman and Sipos (2025), in the United Arab Emirates (UAE), drones are increasingly deployed across a wide range of sectors, including security, urban planning, logistics,

media production, and environmental management. While these technologies enhance operational efficiency and innovation, they simultaneously generate complex legal and ethical challenges, particularly in relation to the protection of individual privacy. The capacity of drones to capture high-resolution imagery, record video footage, and collect real-time spatial data introduces novel forms of surveillance that extend beyond the scope of traditional regulatory frameworks. This evolution necessitates a critical assessment of whether existing legal structures in the UAE are adequately equipped to address the privacy implications arising from drone operations.

Privacy, as a legal concept, broadly encompasses the right of individuals to control access to their personal information, physical spaces, and communications (Gstrein, & Beaulieu 2022). Also, within the UAE legal system, privacy protection is embedded in several legislative instruments, most notably Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes, which criminalises unlawful interception, data collection, and invasions of private life through electronic means. Although this law provides a comprehensive and technology-neutral framework for safeguarding personal data and digital communications, it does not explicitly address the distinctive risks associated with aerial surveillance conducted through drone technologies.

Concurrently, drone operations in the UAE are governed by Federal Decree-Law No. 26 of 2022 Regulating the Civil Use of Drones, which establishes a comprehensive regulatory regime covering registration, licensing, operational permits, airspace zoning, and safety certification under the supervision of the General Civil Aviation Authority (GCAA). While this Decree-Law introduces certain provisions with indirect relevance to privacy such as restrictions on unauthorised installation of imaging devices and the criminalisation of privacy breaches through drone use and its primary orientation remains focused on airspace security, operational safety, and regulatory control. As such, the protection of privacy is treated as a secondary concern, lacking detailed doctrinal articulation in terms of consent, proportionality, data minimisation, and accountability in surveillance practices (Alghafri, & Tubaishat, 2025).

Despite the existence of these parallel legal frameworks, the intersection between drone technology and privacy law remains underdeveloped within the UAE legal system (Zahra, 2025). Aviation regulations primarily emphasise safety, licensing, and national security considerations, whereas cybercrime legislation is oriented toward digital environments, including electronic communications and online platforms. This bifurcated approach produces a fragmented regulatory landscape in which drone-related privacy violations may not be comprehensively addressed, particularly in scenarios involving incidental data capture, persistent aerial monitoring, or the use of drones for quasi-surveillance purposes in densely populated urban environments.

Given the above, this study addresses the absence of a unified and coherent legal framework that explicitly regulates privacy risks arising from drone operations in the UAE. Although existing laws provide partial protection, either through general prohibitions on unlawful data collection or through operational restrictions on drone use. However, there is limited doctrinal integration between these regimes. This lack of integration generates legal uncertainty regarding the scope of individual privacy rights, the allocation of liability, and the effectiveness of enforcement mechanisms in drone-related contexts.

Against this background, the study is guided by the following research questions: What are the legal and regulatory gaps in the UAE framework governing drone-related privacy violations? and How can the current legal framework be reformed to provide more effective protection of privacy in the context of

drone operations? Correspondingly, the research objectives are to examine the adequacy of existing UAE laws in addressing drone-related privacy concerns and to evaluate the extent of fragmentation between aviation regulation and cybercrime legislation in protecting personal privacy against drone surveillance risks.

The significance of this study lies in its contribution to advancing a doctrinal understanding of privacy protection within emerging technological contexts, particularly in relation to drone-enabled surveillance. By critically analysing the interaction between aviation law and cybercrime legislation, the study seeks to identify regulatory deficiencies and propose reform-oriented solutions aimed at enhancing legal coherence and safeguarding individual rights. Additionally, the scope of the study is limited to the UAE legal framework, with a specific focus on the interplay between regulatory control of UAV operations and the protection of privacy rights.

Consequently, this study provides a critical legal evaluation of whether the current regulatory environment in the UAE is sufficiently equipped to address the evolving challenges posed by drone technology, particularly with regard to the protection of individual privacy in an increasingly surveillance-oriented landscape.

2. Research Methodology

This study employs a doctrinal legal research methodology, which involves the systematic examination and interpretation of legal rules, statutes, and doctrinal principles to establish the current position of the law and identify regulatory gaps. Although doctrinal research is traditionally located within legal scholarship, it can be regarded as having a qualitative orientation, as it relies on interpretive analysis of textual materials rather than numerical data. In this regard, Creswell (2014) explains that qualitative research focuses on the interpretive understanding of documents and texts to generate meaning within a specific context. Similarly, Gounder (2012) argues that qualitative doctrinal inquiry enables critical engagement with legal materials to evaluate coherence, consistency, and normative adequacy within legal systems.

The data for this study is derived from secondary sources, including UAE Federal Decree-Laws, policy documents, international legal instruments, and peer-reviewed journal articles, authoritative textbooks, and institutional reports from recognised bodies such as the United Nations and the OECD. These sources were selected based on their legal authority, academic credibility, and relevance to drone regulation and privacy protection. The collected data was subjected to rigorous thematic analysis to identify recurring legal patterns, doctrinal inconsistencies, and regulatory gaps. Braun and Clarke (2006), who are leading scholars of thematic analysis, define it as a structured yet flexible method for identifying, analysing, and reporting patterns within qualitative data.

The study is adopted on Surveillance Theory, not for theoretical testing, but to aid doctrinal analysis and interpretation of legal provisions relating to drone surveillance and privacy protection in the UAE. This ensures that the theory functions as an analytical lens rather than an empirical framework. Overall, this methodological approach provides a systematic and critical doctrinal evaluation of drone-related privacy laws in the UAE while maintaining interpretive rigor and legal coherence.

3. Theoretical Framework,

This study is anchored on Surveillance Theory, to appraise the phenomenon under scrutiny, particularly Michel Foucault's concept of Panopticism (Foucault, 1977). Foucault explains that modern systems of power function through continuous observation, where individuals regulate their behaviour due to the possibility of being watched at any time. The theory is built on several key assumptions. First, visibility is asymmetrical, meaning the observer can see the observed without being seen. Second, surveillance produces self-discipline, as individuals internalise monitoring and adjust behaviour accordingly. Third, power is diffused, operating through multiple institutions and technologies rather than a single authority. Fourth, surveillance is continuous and embedded, extending beyond occasional monitoring to permanent observation. Fifth, technological advancement expands disciplinary control, allowing surveillance to operate across physical and digital environments.

Building on these assumptions, the researcher adopts Surveillance Theory to emphasise that drone technology represents a shift from fixed surveillance systems to mobile, aerial, and pervasive observation mechanisms. It also demonstrates how UAVs extend state and non-state monitoring capacities into everyday spaces, thereby reshaping traditional understandings of privacy. In supporting this position, Lyon (2018) explains that contemporary surveillance is increasingly data-driven and embedded in everyday infrastructures, where visibility becomes a normalised condition of social existence. Similarly, Zuboff (2019) highlights that digital technologies produce new regimes of behavioural prediction and control, reinforcing the expansion of continuous data extraction and monitoring environments.

In the context of this study, Surveillance Theory explains how drones in the UAE function as mobile panopticons that intensify aerial observation beyond traditional regulatory boundaries. This theoretical lens is essential for revealing the doctrinal tension between aviation safety regulation and cybercrime-based privacy protection, as both regimes fail to fully regulate continuous and spatially distributed surveillance enabled by UAVs.

The scientific contribution of this study lies in its doctrinal application of Surveillance Theory to demonstrate that drone technology transforms surveillance from a static legal concern into a continuous and spatially dispersed regulatory challenge. By doing so, the study advances legal scholarship by providing a theoretically grounded explanation of why existing UAE frameworks are insufficient and by strengthening the justification for integrated legal reform addressing drone-enabled privacy violations.

4. Literature Review

4.1 Conceptualising Privacy in the Digital and Surveillance Age

Privacy, within contemporary legal and doctrinal scholarship, is increasingly conceptualised as a multi-dimensional construct that extends beyond traditional notions of seclusion or territorial sanctity (Adeyoju, 2022). Modern legal theory commonly distinguishes between informational privacy, spatial privacy, and surveillance privacy. Informational privacy concerns the ability of individuals to control the collection, use, and dissemination of personal data; spatial privacy relates to the protection of physical environments in which individuals reasonably expect non-interference; while surveillance privacy addresses protection against continuous or systematic monitoring enabled by advanced technologies (Ajala, et al., 2024). This tripartite framework reflects a broader shift from classical privacy doctrine toward a technologically

responsive model of legal protection, particularly within digital governance systems characterised by continuous and transnational data flows.

Within the United Arab Emirates (UAE), privacy protection is predominantly articulated through data-centric and cybercrime-based regulatory frameworks. In particular, Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes adopts a broad definition of personal data as any information relating to an identifiable natural person, whether directly or indirectly (Federal Decree-Law No. 34 of 2021, 2021). This statutory orientation demonstrates a clear emphasis on informational privacy, aligning with global regulatory trends that prioritise personal data as the central object of legal protection in digital environments (United Nations General Assembly, 2022). Such an approach reflects the increasing convergence of privacy and data protection, where safeguarding individual autonomy is primarily achieved through regulating data collection and processing activities.

However, the rapid expansion of emerging technologies has fundamentally altered the scope and intensity of surveillance practices, thereby challenging the adequacy of traditional privacy doctrines. Technologies such as drones, artificial intelligence, facial recognition systems, and geospatial tracking tools have introduced new modalities of data collection that operate across both public and semi-private domains (Jones, 2023). Scholars including Mohsan et al, (2023) opines that at among these, drones represent a particularly significant development due to their capacity to capture real-time visual and spatial data without requiring physical intrusion or fixed infrastructure. Their mobility, persistence, and relative invisibility enable forms of monitoring that are continuous, scalable, and often undetectable. As a result, the distinction between spatial and informational privacy becomes increasingly blurred, as individuals may be subject to data extraction regardless of whether they occupy traditionally protected spaces.

Equally, from a doctrinal perspective, this technological transformation has redefined the nature of privacy intrusion. Conventional legal frameworks were largely designed to address direct and identifiable forms of interference, such as trespass or unauthorised access to private communications. (Aftab,2024). In contrast, contemporary surveillance operates through passive data collection, remote sensing, and algorithmic processing, often without the awareness or participation of the data subject. This phenomenon has been conceptualised as “ambient surveillance,” characterised by continuous observation embedded within everyday environments. As a result, regulatory bodies have increasingly recognised that such developments require a recalibration of legal frameworks to account for ubiquitous data collection systems and automated decision-making infrastructures (OECD, 2019).

Moreover, international governance discourse emphasises that privacy in the digital age extends beyond an individual right to encompass a broader structural function within democratic societies. The widespread deployment of surveillance technologies, including drones in law enforcement, border control, and urban governance, raises fundamental concerns regarding proportionality, necessity, and transparency. These concerns are particularly acute in jurisdictions where legal frameworks do not explicitly address emerging surveillance technologies. The United Nations General Assembly has consistently underscored that digital surveillance measures must comply with established human rights principles, including legality, legitimacy, and effective oversight mechanisms (United Nations General Assembly, 2022).

Accordingly, within this evolving landscape, privacy can no longer be understood solely in terms of protecting physical spaces or preventing misuse of personal data. Instead, it encompasses protection against algorithmic inference, behavioural profiling, and continuous environmental monitoring. The

integration of drone technology into surveillance ecosystems exemplifies this shift, as UAVs facilitate large-scale data collection without clearly defined boundaries between legitimate observation and intrusive monitoring. Thus, Qudus, (2025), noted that, this development exposes a significant regulatory gap in many jurisdictions, including the UAE, where existing cybercrime and data protection laws provide robust safeguards for personal data but do not articulate a sufficiently developed conceptual framework for addressing drone-enabled surveillance. Given the above, a doctrinal tension emerges between rapidly advancing technological capabilities and the scope of existing legal protections, underscoring the need for a more coherent and technologically responsive privacy framework in the digital surveillance age.

4.2 Regulatory Framework Governing Drone Operations in the UAE

The regulatory framework governing drone operations in the United Arab Emirates (UAE) is primarily anchored in Federal Decree-Law No. 26 of 2022 Regulating the Civil Use of Drones, which establishes a comprehensive legal structure for the governance of unmanned aerial vehicles (UAVs) (Federal Decree-Law No. 26 of 2022). The Decree-Law designates the General Civil Aviation Authority (GCAA) as the central regulatory body responsible for oversight, standard-setting, licensing, and enforcement, in coordination with local competent authorities (Regulating, 2026). This framework reflects the UAE's broader aviation governance model, which prioritises airspace safety, national security, and the controlled integration of emerging technologies into existing aviation systems. Consistent with international civil aviation principles, the law seeks to ensure that UAV operations do not compromise public safety or interfere with critical infrastructure and navigational systems.

Similarly, a defining feature of the regulatory regime is its mandatory registration and licensing architecture, which operates as a primary mechanism of state control. Under the Decree-Law, all UAVs must be registered in a unified national register prior to operation, and operators are required to obtain permits and relevant certifications depending on the nature of the activity. The framework distinguishes between recreational, commercial, service, and governmental uses, with increasingly stringent requirements imposed as the operational risk profile escalates. This multi-tiered authorization system comprising registration, operational permits, and safety certification which demonstrates a preventive regulatory approach designed to ensure traceability, accountability, and compliance with aviation safety standards. In doctrinal terms, legality of drone use is thus primarily determined through prior state authorization rather than post hoc assessment of harm (Ahmad et al., 2024).

In addition to licensing requirements, the Law establishes a spatial governance model through the classification of airspace into approved, restricted, and prohibited zones (Blanke, & Shafi, 2024). Hence the UAV operations are permitted only within designated areas, subject to altitude limits, horizontal range restrictions, and compliance with the UAV information map issued by the GCAA. Also, the Sensitive locations including airports, military installations, government facilities, and densely populated areas are subject to heightened restrictions or complete prohibition. While these spatial controls are essential for safeguarding air navigation and national security, they also reveal the regulatory emphasis on physical risk management rather than informational or privacy-related harms. That is why, the primary concern of the framework is where drones may operate, rather than the nature or consequences of the data they collect.

Also, with respect to surveillance capabilities, the law contains limited but noteworthy provisions addressing the use of imaging and data-capturing devices. For instance, Article 9 prohibits the installation or use of cameras and recording equipment on UAVs without prior authorization, while Articles 16 and

18 criminalise the use of drones in a manner that infringes upon the privacy or family life of individuals or facilitates unlawful data collection. These provisions indicate a formal recognition of privacy risks associated with drone technology. However, they remain narrowly framed within a prohibitive and sanction-based logic, rather than constituting a comprehensive regulatory regime governing data practices (Federal Decree-Law No. 26 of 2022). Notably, the law does not articulate detailed standards relating to data collection, storage, retention, processing, or third-party sharing in the context of drone operations. As a result, privacy protection is addressed indirectly and reactively, rather than through a structured and proactive legal framework.

Additionally, the obligations imposed on operators further illustrate the safety-centric orientation of the regulatory system. Operators are required to adhere strictly to authorised flight paths, maintain safe operational distances, comply with technical and procedural requirements, and report incidents such as loss of control or deviation from approved zones. These obligations are primarily designed to prevent physical harm, collisions, and interference with other airspace users. Non-compliance triggers a range of enforcement measures, including administrative sanctions, substantial fines, and, in severe cases, criminal liability. The penalty regime reflects a deterrence-based philosophy aimed at maintaining strict control over airspace usage and mitigating risks to national infrastructure and public safety (Federal Decree-Law No. 26 of 2022).

Consequently, from a critical doctrinal perspective, the UAE drone regulatory framework exhibits a pronounced orientation toward safety, security, and administrative control, with privacy considerations occupying a secondary and underdeveloped position. Although the Law acknowledges the potential for privacy infringement, it does not conceptualise privacy as an independent regulatory objective, nor does it integrate established data protection principles such as consent, purpose limitation, or data minimisation into the governance of UAV operations. Instead, privacy appears as an ancillary concern embedded within broader operational restrictions and criminal prohibitions.

Accordingly, while Federal Decree-Law No. 26 of 2022 Regulating the Civil Use of Drones provides a robust and comprehensive framework for regulating drone operations in terms of licensing, airspace management, and safety compliance, it does not fully engage with the implications of drone technology for informational and spatial privacy. The regulatory focus remains predominantly on how drones are operated, rather than on how the data they generate is governed or how such practices impact individual rights. This structural limitation reinforces the broader argument that the UAE drone regime is fundamentally safety-driven and security-centric, with only limited and insufficiently developed engagement with privacy as a substantive legal concept.

4.3 Legal Protection of Privacy under UAE Cybercrime Legislation

The legal protection of privacy in the United Arab Emirates (UAE) is situated within an increasingly complex regulatory environment shaped by rapid digitalisation and the expansion of data-driven governance. Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes represents a significant legislative development in this regard, as it extends criminal liability to a broad range of cyber-related intrusions, including unlawful access to personal data, interception of communications, and digital surveillance practices. Rather than treating privacy as a purely civil interest, the Decree-Law embeds it

within a criminal enforcement framework, thereby reflecting a securitised approach to data protection that prioritises deterrence and state control over digital harm.

However, scholarly and policy literature suggests that such criminal-law–centred approaches, while effective in addressing overt cyber offences, may not fully capture the structural and systemic dimensions of contemporary privacy risks arising from pervasive data collection and algorithmic processing (Pehlivan, 2024). In this context, global regulatory discourse increasingly frames privacy as a dynamic governance challenge linked to the expansion of digital infrastructures and cross-border data flows rather than merely individual acts of intrusion (OECD, 2019). Similarly, international human rights standards reinforce the view that privacy protection must adapt to technological environments characterised by continuous surveillance and automated decision-making systems, requiring states to ensure proportionality, transparency, and accountability in digital regulation (United Nations General Assembly, 2022).

Additionally, a central feature of the legislation is its detailed prohibition of technologically mediated privacy intrusions. The law criminalises acts such as photographing, recording, or tracking individuals without consent where such conduct infringes upon personal or family life. It further prohibits the acquisition, disclosure, or dissemination of personal data without lawful authorisation. These provisions are significant in that they extend legal protection beyond traditional forms of physical intrusion to encompass digital and electronic modes of surveillance. Consequently, the Decree-Law captures both direct and indirect forms of privacy interference, including cyber-enabled monitoring, data harvesting, and the exploitation of personal information through technological systems.

The legislation also provides robust safeguards in relation to the collection and processing of personal data, thereby reinforcing informational privacy as a central component of the UAE's legal framework. It prohibits the unauthorised use of electronic systems to collect, store, modify, or transmit personal data, including sensitive categories such as financial information, medical records, and geolocation data. By regulating data processing activities, the law reflects alignment with established international data protection principles, including lawful processing, purpose limitation, and data minimisation (OECD, 2019). This indicates that privacy protection under UAE law extends beyond mere confidentiality to encompass control over the entire lifecycle of personal data.

In addition, the Decree-Law explicitly safeguards personal identity, private communications, and location-based information. It criminalises the interception, disclosure, or publication of private communications whether written, audio, or electronic or without legal justification. Similarly, it recognises the sensitivity of spatial privacy by prohibiting unauthorised tracking or disclosure of location data. These provisions demonstrate an awareness that contemporary privacy violations increasingly arise through digital tracking mechanisms and networked surveillance systems rather than through physical intrusion alone.

A defining characteristic of the UAE cybercrime framework is its reliance on a consent-based model of privacy protection (Kulkarni, 2026). Hence, many provisions emphasise the requirement of prior consent or lawful authorisation as a precondition for collecting or processing personal data. This reflects a normative structure in which individual autonomy and informed consent constitute the primary legal basis for legitimising data practices. At the same time, the framework is reinforced by criminal sanctions, indicating that privacy protection is not solely a matter of regulatory compliance but also a subject of penal

enforcement. This dual approach combining consent-based governance with deterrence-based sanctions has positioned the UAE within contemporary models of digital privacy regulation.

Notwithstanding its comprehensive scope, the Decree-Law is fundamentally technology-neutral in its design. While this ensures broad applicability across evolving digital environments, it also results in a lack of specificity in relation to emerging technologies such as unmanned aerial vehicles (UAVs). As argued by Tyshchuk, (2024), that the legislation does not contain dedicated provisions addressing aerial surveillance, drone-based imaging, or the collection of visual and spatial data through remotely operated systems. As a result, the application of its provisions to drone-related activities remains interpretative rather than explicit, creating uncertainty in enforcement and doctrinal clarity.

Also, from a critical standpoint, the UAE cybercrime law provides strong and detailed protections for privacy at a general level, particularly with respect to personal identity, communications, and data processing. However, its technology-neutral structure limits its capacity to engage with the distinctive surveillance capabilities introduced by drones and other autonomous systems. Unlike conventional digital platforms, drones operate at the intersection of physical and informational domains, enabling real-time environmental monitoring and incidental data capture at scale. These characteristics raise unique legal questions that are not fully addressed within the existing framework.

Accordingly, while Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes establishes a robust foundation for privacy protection in principle, it remains insufficiently tailored to the operational realities of drone-enabled surveillance. This limitation reinforces the broader argument of this study that there exists a regulatory mismatch between advanced surveillance technologies and the current conceptualisation of privacy within UAE law, thereby necessitating a more integrated and technology-sensitive legal approach.

4.4 Fragmentation and Legal Gaps in Addressing Drone-Related Privacy Violations

A critical examination of the United Arab Emirates' legal framework reveals a pronounced fragmentation between drone regulation under Federal Decree-Law No. 26 of 2022 Regulating the Civil Use of Drones and privacy protection under Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes. Although both instruments address dimensions of digital governance, they operate in parallel rather than as an integrated regulatory system. The drone law is primarily oriented toward aviation safety, airspace management, and national security, whereas the cybercrime framework focuses on unlawful digital conduct, data misuse, and protection of personal information (Alhajeri, 2022). This structural separation produces limited doctrinal coherence, particularly in relation to surveillance technologies such as drones that simultaneously operate across physical and digital domains. As contemporary regulatory scholarship suggests, fragmented legal regimes are often ill-equipped to address converging technologies that blur the boundaries between data generation, spatial intrusion, and continuous monitoring (OECD, 2019).

A central manifestation of this fragmentation is the absence of explicit cross-referencing or doctrinal integration between the two legal frameworks. The UAV regulatory regime does not systematically incorporate or operationalise the privacy safeguards embedded in cybercrime legislation, nor does the cybercrime law explicitly address drone-enabled data collection or aerial surveillance practices. (McTegg, et al., 2022). Consequently, when drones are used for imaging, tracking, or environmental monitoring,

the applicable legal standard remains uncertain and largely dependent on interpretative extension rather than clear statutory guidance. This lack of integration weakens legal certainty, complicates enforcement, and undermines the consistency of privacy protection in practice (United Nations Human Rights Council, 2023).

A further doctrinal gap arises from the divergence in the foundational logic of legality within the two regimes. Under the drone regulatory framework, legality is primarily determined through prior state authorisation, namely registration, licensing, and operational permits issued by the aviation authority. By contrast, the cybercrime framework is grounded in a consent-based model, where the legitimacy of data collection and processing is contingent upon the consent or lawful authorisation of the individual concerned (European Data Protection Board, 2022). The absence of a harmonised standard results in a regulatory imbalance, whereby state-issued permits may legitimise drone operations without requiring the consent of individuals whose data is captured. This is particularly problematic in public or semi-public environments, where drone surveillance can occur without clear notice or meaningful opportunity for individuals to exercise control over their personal data.

Furthermore, Jordan, (2021) in his scholarly works noted that UAE legal framework lacks a detailed and coherent regime governing the lifecycle of data generated through drone operations. While cybercrime legislation provides general prohibitions against unlawful data processing, it does not specify how aerial data particularly, visual and geospatial information collected by UAVs should be stored, retained, accessed, or shared. This omission is significant given that drone technologies are capable of generating large volumes of high-resolution, persistent data that may be repurposed for behavioural profiling, tracking, or long-term surveillance. In addition, the absence of clear data retention limits and governance standards creates the risk of indefinite storage and secondary use without adequate safeguards, a concern widely recognised in international data protection discourse (European Data Protection Board, 2022).

Similarly, from an enforcement perspective, the UAE framework adopts a predominantly reactive model of regulation. Both the drone law and the cybercrime law rely heavily on post-incident liability, whereby sanctions are imposed only after a violation has occurred. There is limited incorporation of preventive or anticipatory regulatory tools, such as mandatory privacy impact assessments, real-time compliance monitoring, or algorithmic accountability requirements. This reactive orientation is increasingly viewed as insufficient in the context of advanced surveillance technologies, where harm may be continuous, cumulative, and difficult to detect. Emerging international approaches to digital governance emphasise the importance of proactive risk management and ex ante regulatory safeguards to mitigate such risks (United Nations General Assembly, 2022).

Taken together, these doctrinal and structural deficiencies demonstrate that the current UAE legal framework does not provide a fully coherent or effective response to the privacy challenges posed by drone technology. The lack of integration between aviation regulation and privacy law, the divergence between authorisation and consent models, the absence of detailed data governance provisions, the breadth of state exemptions, and the reliance on reactive enforcement collectively create significant gaps in legal protection. These limitations underscore the central argument of this study: while privacy is robustly recognised in principle within UAE cybercrime legislation, it remains insufficiently operationalised and inadequately protected within the specific context of drone-enabled surveillance systems.

5. Discussion and findings

5.1 Conceptualizing Privacy

The findings indicate that privacy in contemporary legal scholarship has shifted from a narrow, territorial concept to a multi-dimensional construct encompassing informational, spatial, and surveillance dimensions (Adeyoju, 2022; Ajala et al., 2024). This conceptual expansion is reinforced by the United Nations General Assembly (2022), which frames privacy as a human rights protection against increasingly pervasive digital surveillance practices. In the UAE, Federal Decree-Law No. 34 of 2021 reflects this global trend by prioritising informational privacy through comprehensive regulation of personal data processing. However, the analysis reveals that this data-centric orientation remains insufficient for addressing surveillance practices enabled by drone technologies, which operate beyond conventional digital boundaries.

The study further finds that unmanned aerial vehicles significantly transform surveillance dynamics by introducing mobile, persistent, and often imperceptible monitoring systems. Jones (2023) and Mohsan et al. (2023) concur that drones extend surveillance into public and semi-private spaces without physical intrusion, thereby blurring the doctrinal distinction between spatial and informational privacy. Aftab (2024) similarly argues that traditional legal frameworks are primarily designed to address direct forms of intrusion and are therefore ill-equipped to regulate algorithmic and passive surveillance systems. This supports the argument that drone technologies generate ambient surveillance environments characterised by continuous data capture.

Moreover, the study emphasises that modern surveillance infrastructures require regulatory recalibration due to their embedded and automated nature. The findings of this study show that UAE regulatory responses remain largely reactive, focusing on sanctions rather than preventive governance mechanisms. Further findings stress that effective surveillance regulation must ensure proportionality, necessity, and transparency, standards that are not fully integrated into drone-specific legal instruments.

In relation to the theory's key assumption of continuous and embedded surveillance, the findings demonstrate that drones institutionalise permanent observation within everyday environments. This aligns with the theoretical proposition that surveillance is no longer episodic but sustained and structurally integrated into social spaces. Consequently, UAV-enabled monitoring in the UAE intensifies the normalisation of surveillance, thereby reinforcing the need for a more coherent and technologically responsive privacy regulatory framework.

5.2 Doctrinal Evaluation and Regulatory Architecture

The analysis reveals that the United Arab Emirates (UAE) drone governance architecture is primarily structured around a safety and security-oriented regulatory logic. Federal Decree-Law No. 26 of 2022 establishes a centralised supervisory system under the General Civil Aviation Authority, which coordinates licensing, enforcement, and operational oversight of unmanned aerial vehicles (UAVs). This institutional arrangement reflects a governance model that privileges airspace integrity, national security, and technological control, while positioning privacy protection as a peripheral concern rather than a central regulatory objective (Regulating, 2026). Consequently, the framework demonstrates a strong compliance-driven structure focused on authorisation and risk containment.

The findings further indicate that the regulatory design is heavily dependent on pre-emptive licensing and registration mechanisms. UAV operations are subject to a tiered authorisation system that differentiates between categories of use and imposes escalating compliance requirements based on perceived operational risk (Ahmad et al., 2024). This approach reflects a preventive governance strategy aimed at ensuring traceability and operational accountability. However, it also reveals a doctrinal emphasis on procedural legality, where lawful drone activity is primarily determined by state approval rather than substantive assessment of privacy implications.

In addition, the spatial regulation of airspace through approved, restricted, and prohibited zones illustrates a territorial model of control that prioritises physical risk management over informational governance (Blanke & Shafi, 2024). While these restrictions are essential for aviation safety, they demonstrate that regulatory attention is concentrated on where drones operate rather than how data is collected, processed, or used. Similarly, although limited provisions address imaging devices and privacy violations, they are framed within prohibitive sanctions rather than comprehensive data governance standards, leaving significant gaps in privacy regulation.

Finally, from the perspective of Surveillance Theory, the findings align with the assumption of visibility asymmetry**,** as the regulatory structure enables state-authorised observation while leaving individuals with limited awareness or control over drone-based monitoring. This reinforces the asymmetrical nature of surveillance embedded within the UAE drone regulatory framework.

5.3 Legal Protection of Privacy

The analysis demonstrates that the UAE's cybercrime framework under Federal Decree-Law No. 34 of 2021 reflects a strong securitised model of privacy protection. The legislation criminalises a wide spectrum of digital intrusions, including unlawful access to personal data, interception of communications, and electronic surveillance practices. This positioning indicates that privacy is primarily protected through penal sanctions rather than civil or administrative remedies, thereby reinforcing a deterrence-oriented governance structure. Pehlivan (2024) similarly observes that cybercrime legislation increasingly functions as an instrument of digital risk control rather than a purely rights-based privacy regime.

Findings further reveal that the UAE framework aligns with global regulatory discourse that conceptualises privacy as a governance issue shaped by data-driven ecosystems. OECD (2019) argues that modern privacy regulation must address systemic data flows rather than isolated breaches, a position reflected in the UAE's emphasis on regulating data processing activities such as collection, storage, and transmission. The legislation's incorporation of principles such as consent, lawful processing, and purpose limitation suggests partial alignment with international data protection standards, although its operationalisation remains fragmented in practice.

In addition, the cybercrime law extends protection to both informational and spatial dimensions of privacy by criminalising unauthorised tracking, recording, and dissemination of personal communications and location data. This indicates doctrinal recognition that privacy violations increasingly occur through digital and geolocation technologies rather than physical intrusion alone. However, as Tyshchuk (2024) notes, the technology-neutral structure of the law limits its responsiveness to emerging surveillance tools such as drones, which generate complex visual and spatial datasets not explicitly regulated under existing provisions.

From a theoretical standpoint, the findings correspond with the assumption that power is diffused across technological systems rather than concentrated in a single authority. The UAE cybercrime regime distributes surveillance control through legal, institutional, and technological mechanisms embedded in digital infrastructures, thereby illustrating how regulatory power operates through interconnected systems of monitoring, enforcement, and data governance.

5.4 Doctrinal Fragmentation

The analysis reveals a clear structural disjunction within the United Arab Emirates (UAE) legal framework governing drones and privacy protection. Federal Decree-Law No. 26 of 2022 and Federal Decree-Law No. 34 of 2021 operate as parallel regulatory regimes without sufficient doctrinal integration. While the former prioritises aviation safety, airspace control, and national security, the latter focuses on cyber-related offences and protection of personal data (Alhajeri, 2022). This regulatory dualism produces fragmented governance, particularly in relation to drone-enabled surveillance, which inherently spans both physical and digital domains. OECD (2019) similarly argues that fragmented legal systems are increasingly inadequate for addressing converging technologies that blur traditional regulatory boundaries.

A key finding is the absence of institutional and normative cross-referencing between both frameworks. The UAV regime does not embed privacy standards from cybercrime legislation, while the cybercrime law does not explicitly regulate aerial data capture. McTegg et al. (2022) observe that such legal silos undermine coherence in technology governance and create interpretative uncertainty. Consequently, enforcement becomes dependent on judicial or administrative interpretation rather than clear statutory direction, thereby weakening legal predictability and consistency (United Nations Human Rights Council, 2023).

The study further finds a doctrinal mismatch in the legal basis of regulation. Drone governance is anchored on prior state authorisation through licensing and registration, whereas cybercrime law relies on individual consent as a basis for lawful data processing (European Data Protection Board, 2022). This divergence creates a regulatory imbalance where lawful drone operations may still result in non-consensual data capture, particularly in public spaces where individuals have limited control over surveillance exposure.

From a theoretical standpoint, these findings align with the assumption of diffused power across institutional and technological systems**,** as regulatory authority is dispersed between aviation regulators and cybercrime enforcement bodies without a unified governance structure. This diffusion explains the persistence of legal gaps and reinforces the study's argument for integrated regulatory reform.

6. Conclusion

This study examines Drone-Related Privacy Violations in the UAE: A Doctrinal Analysis of Regulatory Gaps and Reform Imperatives. The first part of the study covers the conceptualisation of privacy in the digital and surveillance age, explaining how privacy has evolved from a traditional notion of physical seclusion into a multidimensional framework that includes informational, spatial, and surveillance privacy. It highlights how emerging technologies, particularly drones, challenge existing legal doctrines by enabling continuous, remote, and often invisible data collection, thereby blurring the boundaries between physical and digital privacy protections.

The second part delves into the regulatory framework governing drone operations in the UAE, with particular focus on Federal Decree-Law No. 26 of 2022. It demonstrates that the framework is largely safety driven and security oriented, emphasizing licensing, registration, and airspace control. While limited provisions acknowledge privacy concerns, the analysis shows that privacy is treated as a secondary issue and is not comprehensively integrated into the operational or data governance aspects of drone regulation.

The third part addresses the legal protection of privacy under UAE cybercrime legislation, particularly Federal Decree-Law No. 34 of 2021. It establishes that the UAE adopts a strong, consent based and criminal law-oriented approach to privacy protection, covering personal data, communications, and digital surveillance. However, the study reveals that this framework remains technology neutral and lacks specific provisions tailored to drone enabled surveillance, resulting in interpretative uncertainty and limited practical applicability to UAV operations.

The fourth part is allotted to examining the fragmentation and legal gaps within the existing framework. It identifies a lack of doctrinal integration between drone regulation and cybercrime law, inconsistencies between authorization and consent models, and the absence of clear rules governing drone generated data. It further highlights the reliance on reactive enforcement and the limited use of preventive regulatory mechanisms, which collectively weaken effective privacy protection. Consequently, this study adopted doctrinal analysis under the lens of qualitative methodology, and surveillance theory was adopted to aid the analysis.

References

1- Adeyoju, A. (2022). State surveillance, the right to privacy, and why we may need a new international instrument (Doctoral dissertation, University of Saskatchewan).
2- Aftab, S. (2024). The concept of the right to privacy. In Comparative perspectives on the right to privacy: Pakistani and European experiences (pp. 39–98). Springer Nature Switzerland.
3- Ahmad, N., Rahim, F., & Aziz, N. (2024). Can international humanitarian law regulate recent drone strikes?: A case study. JE Asia & Int'l L., 17, 159.
4- Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, O. D. (2024). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. World Journal of Advanced Engineering Technology and Sciences, 11(1), 294–300.
5- Alghafri, B., & Tubaishat, A. (2025). Balancing privacy and security: A comparative analysis of AI-driven surveillance in the UAE and USA. Procedia Computer Science, 257, 142–149.
6- Alhajeri, M. (2022). Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI) (Doctoral dissertation, University of Salford).
7- Al-Zarouni, A., & Farouqi, M. (2022). Regulating unmanned aerial vehicles: A legal framework for global airspace governance. University of Sharjah Journal of Legal Sciences, 23(1).
8- Barman, H., & Sipos, A. (2025). Airport governance in the United Arab Emirates: Latest facilities and future developments. In Aerodrome governance in Asia: Legal and managerial perspectives (pp. 185–209). Springer Nature Singapore.
9- Blanke, G., & Shafi, F. (2024). The United Arab Emirates. Yearbook of Islamic and Middle Eastern Law Online, 23(1), 429–444.

10- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
11- Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage.
12- European Data Protection Board. (2022). Guidelines on data protection impact assessment and risk management. https://edpb.europa.eu
13- Federal Decree-Law No. 26 of 2022 regulating the civil use of drones and activities affiliated with it (United Arab Emirates). (2022). Official Gazette of the United Arab Emirates. https://uaelegislation.gov.ae
14- Federal Decree-Law No. 34 of 2021 on countering rumors and cybercrimes (United Arab Emirates). (2021). Official Gazette of the United Arab Emirates, 2021(714), 1–35. https://uaelegislation.gov.ae
15- Foucault, M. (1977). Discipline and punish: The birth of the prison (A. Sheridan, Trans.). Vintage Books.
16- Gounder, R. (2012). Research methodology and research analysis. PHI Learning.
17- Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1), 3.
18- Hutchinson, T. (2015). Researching and writing in law. Lawbook Company.
19- Jones, H. (2023). The impact of emerging technologies on privacy rights. American Journal of Law and Policy, 1(1), 25–34.
20- Jordan, J. (2021). The future of unmanned combat aerial vehicles: An analysis using the Three Horizons framework. Futures, 134, 102848.
21- Kulkarni, D. (2026). Data privacy and regulatory concerns. In AI, machine learning, and image processing in market research and branding (p. 247).
22- Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.
23- McTegg, S. J., Tarsha Kurdi, F., Simmons, S., & Gharineiat, Z. (2022). Comparative approach of unmanned aerial vehicle restrictions in controlled airspaces. Remote Sensing, 14(4), 822.
24- Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics, 16(1), 109–137.
25- Organisation for Economic Co-operation and Development. (2019). Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies. OECD Publishing. https://doi.org/10.1787/276aaca8-en
26- Pehlivan, C. N. (2024). Data protection in the United Arab Emirates. Global Privacy Law Review, 5(3), 94–96.
27- Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. International Journal of Science and Research Archive, 14(1), 1146–1163.
28- Tyshchuk, V. V. (2024). A review of legal regulation regarding the use of unmanned aerial vehicles for border security and the impact of global technologies. International Comparative Jurisprudence, 10(1), 61–81.
29- United Nations General Assembly. (2022). The right to privacy in the digital age (A/RES/77/211). https://undocs.org/A/RES/77/211

30- United Nations Human Rights Council. (2023). Report on the right to privacy in the digital age (A/HRC/52/37). https://www.ohchr.org
31- Zahra, A. (2025). Algorithmic surveillance and the erosion of privacy: Reconciling national security and human rights in the digital era. In 2025 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 633–638). IEEE.
32- Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.