Legal and Privacy Implications of Unmanned Aircraft Systems (Drones) and AI-Driven Air Traffic Management

Abstract

The rapid convergence of Unmanned Aircraft Systems (UAS) and Artificial Intelligence (AI)-driven Air Traffic Management (ATM) represents a profound paradigm shift in aerospace governance. While the integration of autonomous flight platforms and algorithmic coordination promises unprecedented gains in airspace capacity, logistical efficiency, and operational safety, it destabilises foundational doctrines of aviation law, constitutional privacy, and tort liability. This research paper provides an exhaustive doctrinal, technical, and comparative analysis of the legal and privacy challenges arising from this technological revolution. First, it investigates the crisis in privacy jurisprudence precipitated by low-altitude aerial surveillance, examining how the reasonable expectation of privacy doctrine under the Fourth Amendment intersects with historic property entitlements established in *United States v. Causby* and state legislative enactments. Second, it evaluates the commercial data privacy paradox created by mandatory Remote Identification (Remote ID) regulations, formalising how broadcast telemetry enables third-party surveillance and examining algorithmic obfuscation heuristics to preserve consumer privacy in urban logistics. Third, the paper evaluates international and regional regulatory responses, analysing the limits of Article 8 of the Chicago Convention, the risk-based stratification of European Union regulations including the U-space framework, and strategic oversight initiatives from the United Kingdom and India. Fourth, it deconstructs the legal "responsibility gap" in autonomous operations, formulating a multi-stakeholder risk-and-control accountability mechanism to replace outmoded fault-based models. Fifth, it investigates the operational and cognitive consequences of AI in air traffic control, evaluating human-autonomy teaming, professional liability, and the preservation of Just Culture under International Federation of Air Traffic Controllers' Associations (IFATCA) standards. Finally, it explores cyber-physical architectures integrating Distributed Ledger Technology (DLT), context-aware consensus mechanisms, and Explainable AI (XAI) to secure data provenance and backpropagate trust across autonomous airspace networks.

Keywords: Autonomous Aircraft, Unmanned Aircraft Systems, Air Traffic Management, Remote Identification, Aerial Privacy, Fourth Amendment, U-space, Legal Liability, Explainable AI, Blockchain Consensus.

1. Introduction: The Algorithmic Paradigm Shift in Global Aerospace

Civil aviation has historically operated upon an anthropocentric foundation. International conventions, national safety statutes, and common-law doctrines have presumed the presence of an identifiable human actor a pilot-in-command exercising direct physical control, a licensed aircraft mechanic certifying physical airworthiness, or a certified air traffic controller issuing separation directives. Over the past decade, however, the simultaneous maturation of Unmanned Aircraft Systems (UAS) and Artificial Intelligence (AI) technologies has initiated a systemic transition toward algorithmic aviation. The International Air Transport Association projected that commercial passenger numbers could double to 8.2 billion by 2037,[1] while national aviation authorities anticipate tens of thousands of commercial drones and electric vertical take-off and landing (eVTOL) vehicles entering domestic skies.[2] This exponential growth generates traffic volumes and operational complexities that exceed human perceptual and cognitive limits, making advanced automation not merely an efficiency measure, but an operational necessity.

Addressing these challenges requires moving beyond isolated technical or statutory fixes. This paper develops a comprehensive analysis of the legal, constitutional, and technological mechanisms governing unmanned aviation and algorithmic airspace management, identifying statutory gaps and proposing institutional frameworks to ensure safety, accountability, and individual privacy.

2. Constitutional Privacy and Airspace Property: Fourth Amendment and Common Law Fractures

2.1 Navigable Airspace, Surveillance, and the Reasonable Expectation of Privacy

The domestic proliferation of UAS equipped with multi-sensor payloads ranging from high-resolution optical cameras and thermal imagers to light detection and ranging (LIDAR)

[1] International Air Transport Association. (2018). 20-year passenger forecast. https://www.iata.org

[2] Federal Aviation Administration. (2020). FAA aerospace forecast: Fiscal years 2020–2040. U.S. Department of Transportation.

sensors and automated license plate readers—presents unprecedented threats to spatial privacy.[3] In the United States, judicial assessment of warrantless aerial surveillance has historically centered upon the Fourth Amendment's protection against unreasonable searches.[4] The Supreme Court's jurisprudence, established in the manned aviation era, created an expansive exception for aerial observation conducted from publicly navigable airspace.

In *California v. Ciraolo*,[5] the Supreme Court held that police observation of a fenced backyard curtilage from a fixed-wing aircraft flying at an altitude of 1,000 feet within navigable airspace did not constitute an unlawful search under the Fourth Amendment. Chief Justice Burger reasoned that the Fourth Amendment does not require law enforcement to shield their eyes from activities visible to any member of the flying public. This doctrine was expanded in *Florida v. Riley*,[6] where a plurality of the Court concluded that warrantless helicopter surveillance of a partially covered greenhouse from an altitude of 400 feet did not violate the Fourth Amendment because private and commercial helicopters frequently operate at such altitudes and the observation did not cause physical disruption, excessive noise, or property damage. Similarly, in *Dow Chemical Co. v. United States*,[7] the Court upheld warrantless aerial photography of an extensive 2,000-acre industrial complex from legal airspace, distinguishing industrial facilities from the intimate privacy of the home.

The premise underlying these decisions that an individual lacks a reasonable expectation of privacy against aerial observation if the surveillance occurs from publicly accessible airspace proves deeply problematic when applied to unmanned aircraft. Manned aircraft operations are constrained by high operational costs, fuel limits, pilot fatigue, and safety regulations that prevent persistent, close-proximity loitering. Drones, by contrast, operate at nominal costs, can hover silently at property boundaries, navigate tight urban corridors, and utilize algorithmic facial and object recognition to track targets continuously.[8]

---

[3] U.S. Government Accountability Office. (2020, September 16). Unmanned aircraft systems: Current jurisdictional, property, and privacy legal issues regarding the commercial and recreational use of drones (Report No. B-330570).

[4] Matiteyahu, T. (2015). Drone regulations and Fourth Amendment rights: The interaction of state drone statutes and the reasonable expectation of privacy. Columbia Journal of Law & Social Problems, 48(2), 265–307.

[5] California v. Ciraolo, 476 U.S. 207, 212–214 (1986).

[6] Florida v. Riley, 488 U.S. 445, 450–452 (1989).

[7] Dow Chemical Co. v. United States, 476 U.S. 227, 230–239 (1986).

[8] Kerr, O. S. (2007). Four models of Fourth Amendment protection. Stanford Law Review, 60(2), 503–529.

When modern surveillance jurisprudence is examined, the limitations of *Ciraolo* and *Riley* become apparent. In *Kyllo v. United States*,[9] the Supreme Court held that obtaining information regarding the interior of a home through sense-enhancing technology not in general public use specifically a thermal imaging device used from a public street—constitutes a search presumptively requiring a warrant. Justice Scalia emphasised the necessity of preserving that degree of privacy against government intrusion that existed when the Fourth Amendment was adopted. However, *Kyllo* left ambiguous whether technologies initially deemed exotic lose their constitutional protection once they achieve "general public use," an ambiguity directly relevant as advanced camera drones become ubiquitous consumer goods.

The Court re-anchored Fourth Amendment analysis in proprietary principles in *United States v. Jones*,[10] where Justice Scalia held that physically installing a Global Positioning System (GPS) tracking device on an individual's vehicle to monitor public road movements over 28 days constituted a trespassory search. Crucially, concurring opinions by Justice Sotomayor and Justice Alito recognized that long-term electronic surveillance violates societal expectations of privacy even absent physical trespass, because comprehensive location monitoring reveals an intimate mosaic of familial, political, professional, and religious associations. Drones, however, can conduct sophisticated, persistent tracking across public and private domains without committing a traditional physical trespass on chattels. In *Florida v. Jardines*,[11] the Court reaffirmed that bringing a trained drug-detection dog onto the porch of a home exceeded the customary public license and constituted an unlawful physical search of the curtilage. Justice Kagan's concurrence emphasized that the case could equally have been resolved under the *Katz v. United States* expectation-of-privacy framework,[12] noting that property rights and privacy expectations naturally align because property law reflects societal consensus regarding spaces that must remain free from state interference.

Analogous principles emerge from *Bond v. United States*,[13] where the Supreme Court held that while a bus passenger expects overhead luggage to be touched or moved by others,

---

[9] Kyllo v. United States, 533 U.S. 27, 31–35 (2001).

[10] United States v. Jones, 565 U.S. 400, 404–418 (2012); see also Olmstead v. United States, 277 U.S. 438, 464–466 (1928) (establishing the classical physical-trespass approach to Fourth Amendment searches).

[11] Florida v. Jardines, 569 U.S. 1, 5–12 (2013); see also Oliver v. United States, 466 U.S. 170, 176–181 (1984) (distinguishing protected residential curtilage from unprotected open fields).

[12] Katz v. United States, 389 U.S. 347, 351–353 (1967).

[13] Bond v. United States, 529 U.S. 334, 336–339 (2000).

physical manipulation of an "exploratory" nature violates reasonable expectations of privacy. Applying this reasoning to UAS surveillance suggests a vital distinction: while property owners may expect occasional, incidental drone flyovers, systematic, exploratory loitering and sensor-based data capture violate constitutionally protected expectations of privacy.

2.2 Low-Altitude Airspace and the Tort of Aerial Trespass: Causby, Ad Coelum, and Takings Jurisprudence

The legal status of low-altitude airspace represents a jurisdictional boundary dispute between federal airspace authority and state-recognized real property rights. Historically, English and American common law applied the *ad coelum* doctrine (*cujus est solum, ejus est usque ad coelum* whoever owns the soil owns up to the heavens). The advent of commercial aviation compelled the rejection of this absolute rule. In the landmark decision *United States v. Causby*,[14] the Supreme Court declared the *ad coelum* doctrine obsolete in modern society, recognizing the national airspace as a public highway.

Nevertheless, *Causby* established that landowners retain exclusive ownership of the airspace immediately above their property:

> "The landowner owns at least as much of the space above the ground as he can occupy or use in connection with the land. The fact that he does not occupy it in a physical sense—by the erection of buildings and the like—is not material."[15]

The Court held that frequent, low-altitude military flights passing as low as 83 feet over a commercial chicken farm constituted a direct intrusion upon the enjoyment and use of the land, effecting a compensable taking under the Fifth Amendment. In *Griggs v. County of Allegheny*,[16] the Court reaffirmed this principle, holding an airport owner liable for a constitutional taking when low-altitude takeoffs and landings over residential property severely impaired the owners' use and enjoyment of their land.

The integration of commercial and recreational drones into low-altitude airspace has reignited this property debate. The Federal Aviation Administration (FAA), relying on the Air Commerce Act of 1926, the Federal Aviation Act of 1958, and the FAA Modernization and Reform Act of 2012, asserts preemptive regulatory sovereignty over all navigable airspace in the

---

[14] United States v. Causby, 328 U.S. 256, 260–267 (1946).

[15] United States v. Causby, 328 U.S. 256, 264 (1946).

[16] Griggs v. County of Allegheny, 369 U.S. 84, 88–90 (1962); see also American Law Institute. (1965). Restatement (Second) of Torts (§ 159).

United States, defining navigable airspace down to the surface.[17] Conversely, state and local authorities, real property scholars, and landowners assert that low-altitude airspace (typically below 400 or 500 feet) constitutes private property within the "immediate reaches" defined by *Causby*, prompting state legislatures to enact targeted anti-drone surveillance and aerial trespass statutes.[18]

3. The International and Comparative Regulatory Architecture

3.1 The Chicago Convention Framework: Article 8 and ICAO Global Standards

The international legal framework governing civil aviation is established by the Convention on International Civil Aviation of 1944 (the Chicago Convention).[19] Negotiated decades before the advent of digital flight control, the Convention was structured around manned aircraft operations. Nevertheless, the drafters included visionary language addressing pilotless aircraft under Article 8:

> "No aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization. Each contracting State undertakes to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft."[20]

Article 8 establishes two core international principles: first, sovereign states possess absolute discretion to require and condition the entry of pilotless aircraft into their sovereign airspace; second, states bear a positive international obligation to enforce operational controls that prevent pilotless operations from endangering conventional civil aircraft.

To operationalize these principles, the International Civil Aviation Organization (ICAO) produces Standards and Recommended Practices (SARPs) codified across eighteen technical Annexes to the Chicago Convention, including Annex 2 (Rules of the Air), Annex 6 (Operation

---

[17] Federal Aviation Administration. (2021, January 15). Remote identification of unmanned aircraft (Final Rule, 86 Fed. Reg. 4390; codified at 14 C.F.R. pt. 89); see also Ding, G., Berke, A., Degue, K. H., Gopalakrishnan, K., Li, M. Z., & Balakrishnan, H. (2023). Routing with privacy for drone package delivery systems. arXiv. https://arxiv.org/abs/2303.00123

[18] See Freedom from Drone Surveillance Act, 725 Ill. Comp. Stat. Ann. 167/1–167/35 (2013); Freedom from Unwanted Surveillance Act, Fla. Stat. Ann. § 934.50 (2013); Idaho Code Ann. § 21-213 (2013); Tex. Gov't Code Ann. §§ 423.001–423.008 (2013); Or. Rev. Stat. Ann. §§ 837.300–837.390 (2013).

[19] Convention on International Civil Aviation, art. 8, December 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

[20] Convention on International Civil Aviation, art. 8, December 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

of Aircraft), and Annex 8 (Airworthiness of Aircraft). While ICAO's foundational Circular 328 on Unmanned Aircraft Systems[21] and its Manual on Remotely Piloted Aircraft Systems (Doc 10019)[22] provided initial guidance for remotely piloted operations, international civil aviation bodies recognize that these frameworks do not resolve the unique challenges of machine autonomy.

At the 42nd Session of the ICAO Assembly, an executive working paper presented by Singapore, co-authored by Thailand, and co-sponsored by Canada, China, and the Republic of Korea (A42-WP/234) highlighted that the rapid introduction of probabilistic, opaque machine learning algorithms creates acute challenges for safety oversight, institutional accountability, and international interoperability.[23] The working paper emphasized that fragmented national data architectures and divergent regulatory standards risk undermining global ATM harmonisation. While existing data exchange protocols such as the Aeronautical Information Exchange Model (AIXM), the Flight Information Exchange Model (FIXM), and the ICAO Meteorological Information Exchange Model (IWXXM) provide a digital foundation, global aviation readiness demands standardized governance, liability distribution rules, and certified talent pipelines.[24]

In the United Kingdom, the Civil Aviation Authority (CAA) formulated a strategic regulatory approach to emerging AI-enabled automation, articulated in Civil Aviation Publication (CAP) 3064A.[25] The CAA strategy aligns aviation oversight with the UK

[21] International Civil Aviation Organization. (2011). Unmanned aircraft systems (UAS) (Circular 328-AN/190).

[22] International Civil Aviation Organization. (2015). Manual on remotely piloted aircraft systems (RPAS) (1st ed., Doc 10019-AN/507).

[23] International Civil Aviation Organization. (2025, July 29). Responsible and strategic integration of artificial intelligence in international civil aviation (Working Paper A42-WP/234, Assembly 42nd Session, Executive Committee).

[24] See also European Commission. (2019, May 24). Commission Implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft. Official Journal of the European Union, L 152, 45–71; European Commission. (2019, March 12). Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Official Journal of the European Union, L 152, 1–40; European Commission. (2021, April 22). Commission Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space. Official Journal of the European Union, L 139, 161–183; European Commission. (2023, October 27). Commission Implementing Regulation (EU) 2023/203 laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for the management of information security risks. Official Journal of the European Union, L 31, 1–40; European Union Aviation Safety Agency. (2023, May). Artificial intelligence roadmap 2.0: A human-centric approach to AI in aviation; European Union Aviation Safety Agency. (2024, March). Guidance for Level 1 & 2 machine learning applications (EASA Concept Paper, Issue 02).

[25] Civil Aviation Authority of the United Kingdom. (2024, November). Part A: Strategy for regulating AI and advanced automation in aerospace (Civil Aviation Publication CAP3064A).

Government's broader pro-innovation framework established by the Department for Science, Innovation and Technology (DSIT), which centers on five overarching regulatory principles:[26]

1. Safety, Security, and Robustness: Ensuring AI systems function reliably and resist adversarial interference.

2. Appropriate Transparency and Explainability: Mandating that algorithmic outputs can be interpreted and validated by human supervisors.

3. Fairness: Preventing systemic bias in airspace access, flight routing, and operational prioritization.

4. Accountability and Governance: Establishing clear corporate and individual oversight channels for autonomous systems.

5. Contestability and Redress: Providing formal administrative and legal mechanisms to dispute automated decisions.

4. Liability, Causation, and the "Responsibility Gap" in Autonomous Systems

4.1 From Pilot Fault to Software Defect: The Erosion of Fault-Based Tort Regimes

The central legal challenge posed by autonomous aviation is the breakdown of traditional fault-based tort liability. In conventional civil aviation, liability for accidents can almost invariably be anchored to human negligence. The pilot-in-command, carrier, or air traffic controller owes a legal duty of care to passengers and third parties on the surface; breach of that duty, directly causing harm, triggers liability under negligence or statutory strict liability regimes. International treaties such as the Warsaw Convention of 1929, the Montreal Convention of 1999 for passenger carrier liability,[27] and the Rome Convention of 1952 for third-party surface damage presume an identifiable human operational entity.[28]

When an autonomous aircraft guided by machine learning algorithms executes an unexpected course correction, fails to detect an airborne obstacle, or crashes due to anomalous

[26] Civil Aviation Authority of the United Kingdom. (2024). 5 principles for building trust in AI systems (Civil Aviation Publication CAP2970).

[27] Convention for the Unification of Certain Rules for International Carriage by Air, May 28, 1999, 2242 U.N.T.S. 309.

[28] Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface, October 7, 1952, 310 U.N.T.S. 181.

sensor processing, traditional fault concepts fail. Legal and philosophical scholars, notably Andreas Matthias, characterize this structural dilemma as the "responsibility gap":[29]

> When an operator or manufacturer deploys a machine learning system that independently optimizes its decision-making through environmental interaction and non-linear data processing, an outcome may occur that no human designer could predict or prevent. Consequently, holding the human operator liable under fault principles is legally unjust, yet treating the machine as an unaccountable entity leaves the victim without a remedy.[30]

Holding the remote operator liable for every autonomous decision imposes an unfair burden of strict liability upon a user who possessed no meaningful ability to control the system. Conversely, absolving the operator without providing clear recourse against manufacturers or software developers creates an unacceptable accountability vacuum. The legal dispute therefore shifts from human negligence (breach of standard of care) to product liability (systemic defect in design, manufacture, or algorithmic performance). Under the *Restatement (Third) of Torts: Products Liability*,[31] as well as the modern European Union Product Liability Directive (Directive 2024/2853),[32] software and digital files are increasingly treated as products. If an autonomous navigation algorithm contains a design defect, lack of robustness, or inadequate fail-safe mechanisms that contribute to an accident, the injured party must pursue complex product liability litigation against technology suppliers, software houses, or airframe integrators.

5. The culture and dilemma

5.1 The Just Culture Dilemma and Professional Liability Under Automation

The automation of air traffic control creates acute legal dilemmas concerning professional controller liability. Under established aviation safety frameworks, accident investigation relies upon the principle of "Just Culture"—an environment where front-line

[29] Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. Ethics and Information Technology, 6(3), 175–183; see also Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468.

[30] Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. Ethics and Information Technology, 6(3), 175–183.

[31] American Law Institute. (1998). Restatement (Third) of Torts: Products liability.

[32] European Parliament & Council of the European Union. (2024, October 23). Directive (EU) 2024/2853 on liability for defective products. Official Journal of the European Union, L 2853, 1–28.

operators are encouraged to report errors and safety occurrences without fear of prosecution, distinguishing between honest, human mistakes and gross negligence or willful misconduct.[33]

When AI algorithms generate conflict-resolution advisories, the allocation of legal responsibility becomes highly uncertain. IFATCA Technical and Professional Manual (TPM) policy AAS 1.20 explicitly establishes that:

> "Artificial Intelligence and/or Machine Learning based systems should only be implemented as decision support systems and shall not replace the decision of the ATCO... ATCO's responsibility shall be proportionally decreased in accordance with the level of automation and their ability to intervene and control automated systems."[34]

Furthermore, under IFATCA policy WC 10.2.5, a controller is not held responsible when an automated system's resolution advisory results in a loss of aircraft separation.[35]

However, a severe legal dilemma arises when an automated system issues a resolution advisory that the human controller doubts. If the controller chooses to disregard the machine's advisory based on professional intuition, and an incident occurs, existing legal regimes are predisposed to find the human controller negligent for overriding an automated safety system. Conversely, if the controller passively accepts an erroneous algorithmic advisory that results in a collision, the controller faces liability for failing to maintain situational vigilance. In practice, front-line controllers fear they will become legal "moral crumple zones"—bearing ultimate legal and criminal culpability for systemic algorithmic failures while lacking the real-time cognitive capability to understand or override opaque machine decisions.[36]

To preserve Just Culture in algorithmic airspace, legal frameworks must formally decouple controller liability from automated system failures. As long as controllers lack

---

[33] International Federation of Air Traffic Controllers' Associations. (2025, April 28–May 2). ATCO skills with the use of artificial intelligence and legal liability (Working Paper No. 157, Agenda Item C.6.11, 64th Annual Conference, Abu Dhabi, UAE).

[34] International Federation of Air Traffic Controllers' Associations. (2024). Technical and professional manual (TPM) (Policy AAS 1.20).

[35] International Federation of Air Traffic Controllers' Associations. (2024). Technical and professional manual (TPM) (Policy WC 10.2.5).

[36] International Federation of Air Traffic Controllers' Associations. (2025, April 28–May 2). ATCO skills with the use of artificial intelligence and legal liability (Working Paper No. 157, Agenda Item C.6.11, 64th Annual Conference, Abu Dhabi, UAE).

complete, transparent visibility into why an AI system generates a specific directive,[37] they cannot legally be held to a standard of absolute operational liability.

5.2 Skill Fade, Training Mandates, and Re-Evaluating System Failure Protocols

Extensive automation introduces significant human factors risks, most notably cognitive deskilling and "skill fade." In human factors surveys evaluating workers' reliance on automated tools, 78% of respondents indicated that heavy dependence upon AI systems limits creative engagement, problem-solving dexterity, and sustained vigilance.[38] In air traffic control, if human operators spend years supervising automated vectoring without actively calculating separation maneuvers, their instinctive spatial skills inevitably degrade.

In the event of an abrupt algorithmic failure—caused by a cyber incident, communication link disruption, or edge-case sensor confusion—the human controller is expected to step in and assume manual control of an intensely congested airspace sector. However, transferring a controller from low-arousal supervisory monitoring to high-stress emergency intervention within seconds is cognitively impossible without catastrophic error risk. To mitigate this operational vulnerability, IFATCA policy TRNG 9.5.1 mandates that controllers participate in rigorous annual refresher training courses specifically designed to maintain manual separation abilities and operational dexterity across degraded-mode scenarios.[39] Furthermore, aviation safety policy requires that whenever an automated ATM tool fails, the Air Navigation Service Provider (ANSP) must immediately restrict total airspace capacity and sector traffic volume to levels that can be safely managed by the available human team using conventional procedural control.

---

[37] See Axon, L., Panagiotakopoulos, D., Ayo, S., Sanchez-Hernandez, C., Zong, Y., Brown, S., Zhang, L., Goldsmith, M., Creese, S., & Guo, W. (2023). Securing autonomous air traffic management: Blockchain networks driven by explainable AI. IEEE Aerospace and Electronic Systems Magazine. https://arxiv.org/abs/2304.14095

[38] International Federation of Air Traffic Controllers' Associations. (2025, April 28–May 2). ATCO skills with the use of artificial intelligence and legal liability (Working Paper No. 157, Agenda Item C.6.11, 64th Annual Conference, Abu Dhabi, UAE).

[39] International Federation of Air Traffic Controllers' Associations. (2024). Technical and professional manual (TPM) (Policies TRNG 9.2.5 & TRNG 9.5.1).

6.References:

American Law Institute. (1965). *Restatement (Second) of Torts* (§ 159).

American Law Institute. (1998). *Restatement (Third) of Torts: Products liability*.

Axon, L., Panagiotakopoulos, D., Ayo, S., Sanchez-Hernandez, C., Zong, Y., Brown, S., Zhang, L., Goldsmith, M., Creese, S., & Guo, W. (2023). Securing autonomous air traffic management: Blockchain networks driven by explainable AI. *IEEE Aerospace and Electronic Systems Magazine*. https://arxiv.org/abs/2304.14095

The Bharatiya Vayuyan Adhiniyam, No. 32 of 2024, Acts of Parliament, 2024 (India).

Bond v. United States, 529 U.S. 334 (2000).

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, *13*(4), 447–468.

California v. Ciraolo, 476 U.S. 207 (1986).

Civil Aviation Authority of the United Kingdom. (2024). *5 principles for building trust in AI systems* (Civil Aviation Publication CAP2970).

Civil Aviation Authority of the United Kingdom. (2024, November). *Part A: Strategy for regulating AI and advanced automation in aerospace* (Civil Aviation Publication CAP3064A).

Convention for the Unification of Certain Rules for International Carriage by Air, May 28, 1999, 2242 U.N.T.S. 309.

Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface, October 7, 1952, 310 U.N.T.S. 181.

Convention on International Civil Aviation, art. 8, December 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

Ding, G., Berke, A., Degue, K. H., Gopalakrishnan, K., Li, M. Z., & Balakrishnan, H. (2023). *Routing with privacy for drone package delivery systems*. arXiv. https://arxiv.org/abs/2303.00123

Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

European Commission. (2019, March 12). Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. *Official Journal of the European Union*, *L 152*, 1–40.

European Commission. (2019, May 24). Commission Implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft. *Official Journal of the European Union*, *L 152*, 45–71.

European Commission. (2021, April 22). Commission Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space. *Official Journal of the European Union*, *L 139*, 161–183.

European Commission. (2023, October 27). Commission Implementing Regulation (EU) 2023/203 laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for the management of information security risks. *Official Journal of the European Union*, *L 31*, 1–40.

European Parliament & Council of the European Union. (2024, October 23). Directive (EU) 2024/2853 on liability for defective products. *Official Journal of the European Union*, *L 2853*, 1–28.

European Union Aviation Safety Agency. (2023, May). *Artificial intelligence roadmap 2.0: A human-centric approach to AI in aviation*.

European Union Aviation Safety Agency. (2024, March). *Guidance for Level 1 & 2 machine learning applications* (EASA Concept Paper, Issue 02).

Federal Aviation Administration. (2020). *FAA forecast: Fiscal years 2020–2040*. U.S. Department of Transportation.

Federal Aviation Administration. (2021, January 15). Remote identification of unmanned aircraft (Final Rule, 86 Fed. Reg. 4390; codified at 14 C.F.R. pt. 89).

Florida v. Jardines, 569 U.S. 1 (2013).

Florida v. Riley, 488 U.S. 445 (1989).

Freedom from Drone Surveillance Act, 725 Ill. Comp. Stat. Ann. 167/1–167/35 (2013).

Freedom from Unwanted Surveillance Act, Fla. Stat. Ann. § 934.50 (2013).

Griggs v. County of Allegheny, 369 U.S. 84 (1962).

Idaho Code Ann. § 21-213 (2013).

International Air Transport Association. (2018). *20-year passenger forecast*.

International Civil Aviation Organization. (2011). *Unmanned aircraft systems (UAS)* (Circular 328-AN/190).

International Civil Aviation Organization. (2015). *Manual on remotely piloted aircraft systems (RPAS)* (1st ed., Doc 10019-AN/507).

International Civil Aviation Organization. (2025, July 29). *Responsible and strategic integration of artificial intelligence in international civil aviation* (Working Paper A42-WP/234, Assembly 42nd Session, Executive Committee).

International Federation of Air Traffic Controllers' Associations. (2024). *Technical and professional manual (TPM)* (Policies AAS 1.20, WC 10.2.5, TRNG 9.2.5, & TRNG 9.5.1).

International Federation of Air Traffic Controllers' Associations. (2025, April 28–May 2). *ATCO skills with the use of artificial intelligence and legal liability* (Working Paper No. 157, Agenda Item C.6.11, 64th Annual Conference, Abu Dhabi, UAE).

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O. S. (2007). Four models of Fourth Amendment protection. *Stanford Law Review*, *60*(2), 503–529.

Kyllo v. United States, 533 U.S. 27 (2001).

Law Commission of England and Wales. (2026, May 20). *Aviation autonomy: Final report* (Law Com No. 412).

Matiteyahu, T. (2015). Drone regulations and Fourth Amendment rights: The interaction of state drone statutes and the reasonable expectation of privacy. *Columbia Journal of Law & Social Problems*, *48*(2), 265–307.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, *6*(3), 175–183.

Ministry of Civil Aviation. (2021, August 25). *The Drone Rules, 2021* (G.S.R. 589(E)). Gazette of India.

Oliver v. United States, 466 U.S. 170 (1984).

Olmstead v. United States, 277 U.S. 438 (1928).

Or. Rev. Stat. Ann. §§ 837.300–837.390 (2013).

Raahul, T. R. (2026). Regulating autonomous aircraft: Legal challenges of artificial intelligence-driven aviation. *Advanced International Journal for Research*, *3*(1), 1–45.

RTCA Inc. (2011). *DO-178C: Software considerations in airborne systems and equipment certification*.

RTCA Inc. & EUROCAE. (2014). *DO-326A / ED-202A: Airworthiness security process specification*.

Tex. Gov't Code Ann. §§ 423.001–423.008 (2013).

U.S. Government Accountability Office. (2020, September 16). *Unmanned aircraft systems: Current jurisdictional, property, and privacy legal issues regarding the commercial and recreational use of drones* (Report No. B-330570).

United States v. Causby, 328 U.S. 256 (1946).

United States v. Jones, 565 U.S. 400 (2012).