

MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 20 | NUMBER 2 | FALL 2026 | ISSN 1802-5943

PEER REVIEWED



CONTENTS:

MESARČÍK | NOMANI | RABABA | AL-AHMAD | MUKHTAR |
MUHAMMAD | AMIN | SCHAFER | RAUDSEPP | KIKERPILL

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology

issued by Institute of Law and Technology

Faculty of Law, Masaryk University

www.mu.jlt.law.muni.cz

Editor-in-Chief

Jakub Harašta, Masaryk University, Brno

Deputy Editor-in-Chief

Ondřej Böhm, Masaryk University, Brno

Founding Editor

Radim Polčák, Masaryk University, Brno

Editorial Board

Tomáš Abelovský, Swiss Re, Zurich

Zsolt Balogh, Corvinus University, Budapest

Michael Bogdan, University of Lund

Joseph A. Cannataci, University of Malta | University of Groningen

Josef Donát, ROWAN LEGAL, Prague

Julia Hörnle, Queen Mary University of London

Josef Kotásek, Masaryk University, Brno

Leonhard Reis, University of Vienna

Naděžda Rozehnalová, Masaryk University, Brno

Vladimír Smejkal, Brno University of Technology

Martin Škop, Masaryk University, Brno

Dan Jerker B. Svantesson, Bond University, Gold Coast

Markéta Trimble, UNLV William S. Boyd School of Law

Andreas Wiebe, Georg-August-Universität Göttingen

Aleš Završnik, University of Ljubljana

Editors

Tina Mizerová, Andrej Krištofik

Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o. (<https://rowan.legal>)

Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions

Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)

listed in Scopus (www.scopus.com)

reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 20 | NUMBER 2 | FALL 2026

LIST OF ARTICLES

- Matúš Mesarčík:** Esports and the Digital Services Act: Functional Classification of Gaming, Tournament and Streaming Services.....153
- Sumaiya Firoz Nomani, Mohammad Rababa, Hussain Al-Ahmad, Husameldin Mukhtar, Nasiruddeen Muhammad, Saad Ali Amin, Burkhard Schafer:** Data Protection and Cybersecurity Governance for eVTOL Systems in the UAE: Comparative Lessons from the EU and US.....185
- Lee Raudsepp, Kristjan Kikerpill:** Shut Down, Sued, and Silenced: Strategic Suppression Tactics of Technology Corporations.....221

DOI 10.5817/MUJLT2026-42629

ESPORTS AND THE DIGITAL SERVICES ACT: FUNCTIONAL CLASSIFICATION OF GAMING, TOURNAMENT AND STREAMING SERVICES *

by

MATÚŠ MESARČÍK [†]

Electronic sports (eSports) have developed into a complex digital ecosystem combining competitive gameplay, private governance, live broadcasting, user communication, monetisation, and platform-based audience interaction. This article examines how the EU Digital Services Act (DSA) applies to that ecosystem not as a sectoral regulation of eSports, but through the DSA's functional categories of intermediary services, hosting services, online platforms, and very large online platforms. The article argues that the central legal difficulty is one of functional segmentation meaning that the game itself, player accounts, in-game communication tools, user generated content (UGC) workshops, tournament portals, live chats, streaming interfaces, and recommender systems may attribute different legal labelling. Streaming platforms and public UGC infrastructures present the clearest cases of platform regulation, while publishers and tournament organisers require more careful analysis because many of their functions may be ancillary, closed, or attributable to the provider rather than to recipients of the service. The article therefore maps the boundaries of DSA applicability in eSports and identifies specific compliance questions concerning moderation of live events, statements of reasons during short-lived competitions, public fan interaction tools, minors in competitive environments, recommender systems for eSports content, and the relationship between DSA obligations and private integrity governance.

* Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I03-03-V04-00345.

[†] doc. JUDr. Matúš Mesarčík, PhD., LL.M, the Slovak Academy of Sciences of the Slovak Republic: Researcher; Comenius University Bratislava, Faculty of Law: Associate Professor. E-mail: matus.mesarcik@flaw.uniba.sk; ORCID: 0000-0003-3311-5333.

KEY WORDS

electronic sports, video games, Digital Services Act, minors, design

1. INTRODUCTION

Electronic sports (eSports) have transformed from a niche subculture into a global industry, attracting millions of players and spectators. Competitive gaming tournaments now rival traditional sports in terms of viewership, with events such as the League of Legends World Championship and The International (Dota 2) drawing audiences in the tens of millions.¹ The economic significance of eSports is also undeniable, with the industry projected to surpass €2 billion in annual revenue by 2025, driven by sponsorships, media rights, and digital content sales.² Online games are also booming on the European market (over €23 billion in annual revenue) and a mainstream pastime for half of Europeans.³

As eSports continue to grow, their regulation remains a complex and evolving issue. Unlike traditional sports, where governance structures are well-established, eSports competitions are largely shaped by game publishers, online platforms, and tournament organizers. The European Union's Digital Services Act (DSA)⁴ introduces new regulatory obligations for digital platforms, raising critical questions about how eSports games and competitions fit into this framework. From content moderation and algorithmic transparency to the protection of minors and limits on manipulative interface design, the DSA may affect specific intermediary functions within the eSports ecosystem. It does not, however, regulate eSports as such, nor does it automatically apply to gameplay mechanics, balance decisions, or official game content.

This paper argues that eSports platforms and stakeholders occupy a distinctive position within the DSA framework. Game publishers, tournament organisers, and streaming platforms all provide digital services, but their roles and potential regulatory obligations differ substantially due to the regulatory regime. Understanding these distinctions is crucial for assessing how the DSA may aid to shape eSports governance in general.

¹ MordorIntelligence. (2023) eSports Market. Available from: <https://www.mordorintelligence.com/industry-reports/eSports-market> [Accessed 27 May 2025].

² PwC. (2023) Future of eSports. Available from: <https://www.strategyand.pwc.com/ml/en/strategic-foresight/sector-strategies/media/future-of-eSports.html> [Accessed 27 May 2025].

³ European Parliament. (2022) Resolution on the Role of Video Games in the European Economy: Challenges and Opportunities. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022IP0388> [Accessed 27 May 2025].

⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022, p. 1–102.

The article therefore proceeds from a functional rather than institutional premise. The relevant question is not whether a publisher, tournament organiser, or streaming service is an eSports platform in general, but whether a particular function of that service stores information provided by recipients, disseminates such information to the public, or reaches the threshold for enhanced DSA obligations. This distinction is especially important in eSports because the same ecosystem may contain official game content, content created by players, private team communication, public chat, tournament administration, live broadcasting, and audience interaction resembling classic social media life.

The paper therefore addresses three interrelated research questions:

- How should services with mixed functions within the eSports ecosystem be classified under the DSA's categories of intermediary services, hosting services, online platforms, and very large online platforms?
- When do functions related to eSports such as public chats, UGC workshops, replay-sharing tools, fan zones, tournament portals, and streaming interfaces amount to public dissemination of user-generated information rather than minor or purely ancillary features?
- How do selected DSA obligations apply differently to publishers, tournament organisers, and streaming platforms once these functions are separated, particularly in relation to live-event moderation, statements of reasons, protection of minors, interface design, recommender systems, and private integrity governance?

The current scholarship on the DSA is now grounded by authoritative volumes that outline the regulation's functional methodology, its graduated obligations and offers comprehensive statutory interpretation, contextualize the DSA within the framework of EU constitutional principles, and highlight specific duties related to important actors instead of sector-based categorizations.⁵ Growing body of literature on platform governance and content moderation under the DSA highlights the shift in the EU law from ex-post liability to proceduralised due process, emphasizing clear terms, accessible notice-and-action, statements of reasons, and transparency

⁵ Husovec, M. (2024) *Principles of Digital Services Act*. Oxford: Oxford University Press and Wilman, F., Kaleda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press.

databases⁶ and the role of terms and conditions in terms of protection of fundamental rights and freedoms.⁷ Recent literature on DSA obligations related to minors increased⁸ after the Commission's 2025 guidelines,⁹ which set context-specific compliance rules. The European Data Protection Board¹⁰ raised concerns about GDPR and age-assurance, while UNICEF¹¹ and earlier parental-control research provide risk analyses for interactive platforms.¹² In terms of dark patterns and manipulative designs, the literature provides a taxonomy of manipulative design¹³ and risks towards minors¹⁴ while analytical reports extend the analysis to policies.¹⁵ Further research on recommender-system transparency defines the meaning of "main parameters" and non-profiling options¹⁶ and proposes "constructive optimisation" to align algorithmic design with autonomy¹⁷ and technical

⁶ Wolters, P. and Gellert, R. (2023) 'Towards a Better Notice-and-Action Mechanism in the DSA'. JIPITEC, 14, p. 403 and Keller, D. (2022) 'The DSA's Industrial Model for Content Moderation'. *VerfBlog*.

⁷ Quintais, J. (2023) 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation'. *German Law Journal*.

⁸ See Chawki, M. (2025) 'AI Moderation and Legal Frameworks in Child-Centric Social Media: A Case Study of Roblox'. *Laws*, 14, p. 29. Available from: <https://doi.org/10.3390/laws14030029> [Accessed 27 May 2025] or Kusters, L. and Gstrein, O. J. (2023) 'TikTok and Transparency Obligations in the EU Digital Services Act (DSA) – A Scoping Review'. *Zeitschrift für Europarechtliche Studien (ZEuS)*, 01/2024, pp. 110–132. Available from: <https://ssrn.com/abstract=4652543> or <http://dx.doi.org/10.2139/ssrn.4652543> [Accessed 2 December 2023].

⁹ European Commission. (2025) *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(1) of Regulation (EU) 2022/2065, C/2025/5519*. [Accessed 27 May 2025].

¹⁰ European Data Protection Board. (2025) *Statement 1/2025 on Age Assurance*. Adopted on 11 February 2025. Available from: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf [Accessed 27 May 2025].

¹¹ UNICEF. (2020) *Online gaming: respecting and supporting children's rights and well-being*. Available from: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming> [Accessed 27 May 2025].

¹² ESports Integrity Commission. (2019) *The Importance of Child Protection in eSports*. Available from: <https://esic.gg/industry-update/the-importance-of-child-protection-in-eSports/> [Accessed 27 May 2025].

¹³ Luguri, B. and Strahilevitz, L. (2021) Shining a Light on Dark Patterns. *Journal of Legal Analysis*.

¹⁴ Rossi, A. et al. (2024) Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. *Computer Law & Security Review*, 55, 106031. Available from: <https://www.sciencedirect.com/science/article/pii/S0267364924000979?via=ihub> [Accessed 27 May 2025].

¹⁵ OECD. (2022) *Dark Commercial Patterns*.

¹⁶ Busch, C. (2023) 'From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation'. In: Milano, S. and Taddeo, M. (eds) *Recommender Systems: Legal and Ethical Issues*. Cham: Springer, pp. 31–54. Available from: https://doi.org/10.1007/978-3-031-34804-4_3 [Accessed 29 June 2026].

¹⁷ Naudts, A., Helberger, N., Sax, M. and Veale, M. (2024) 'Toward Constructive Optimisation'.

game-studies work¹⁸ illustrates these mechanisms in play environments. By contrast, eSports research though rich in analyses of governance, integrity, and monetisation has not yet applied DSA obligations to this sector. Existing studies describe eSports institutionally¹⁹ but do not classify stakeholders or map the specific compliance requirements.

By situating above mentioned questions within ongoing doctrinal debates, the paper aims to make two contributions. First, it provides a structured, theoretically informed mapping of eSports stakeholders under the DSA, addressing an overlooked but doctrinally significant case study in platform regulation. Second, it uses the eSports ecosystem to illuminate broader tensions in the DSA's application to mixed-function digital services, including the integration of user-generated content into official game environments, the boundaries of obligations related to design of digital services, and the protection of minors in competitive gaming. This paper therefore contributes both to the literature on the DSA and to emerging regulatory scholarship on competitive digital environments.

The article's contribution is therefore not the claim that platforms related to gaming can fall within the DSA, a point already recognised in broader debates surrounding EU platform regulation. Its contribution is narrower as it uses eSports as a case study to clarify the boundary between controlled game environments by providers and intermediary functions drove by recipients of services. This boundary is particularly difficult in eSports because competitive games are embedded in surrounding infrastructures of accounts, chats, replays, public rankings, UGC markets, tournament portals, and live-streaming services. The article argues that DSA obligations should be attached to these functions only where the statutory criteria are met.

The analysis proceeds by mapping the eSports stakeholder landscape, examining the applicability of the DSA to these actors, and exploring the practical implications of key obligations. Conclusions are provided at the end of the paper.

¹⁸ Sifa, R., Zhai, K., Pawlakos, E. et al. (2018) 'Controlling the Crucible: A Novel PvP Recommender Systems Framework for Destiny'. In: *Proceedings of Australian Computer Science Week, Interactive Entertainment*. ACM.

¹⁹ Taylor, T.L. (2012) *Raising the Stakes: E-Sports and the Professionalization of Computer Gaming*. Cambridge, MA: MIT Press; Jenny, S.E., Manning, R.D., Keiper, M.C. and Olrich, T.W. (2017) 'Virtual(ly) Athletes: Where eSports Fit Within the Definition of "Sport"'. *Quest*, 69, p. 1; Parry, J. (2018) 'E-sports Are Not Sports'. *Sports, Ethics and Philosophy*, 13, p. 3; Naraine, M.L. (2021) 'Actually, ESports Is Sport: A Response to Parry's (2019) Misguided View'. *Sports Innovation Journal*, 2, p. 33; Martinelli, J. (2019) 'The Challenges of Implementing a Governing Body for Regulating ESports'. *University of Miami International and Comparative Law Review*, 26, p. 499; Leahy, D. (2022) 'Rocking the Boat: Loot Boxes in Online Digital Games, the Regulatory Challenge, and the EU's Unfair Commercial Practices Directive'. *Journal of Consumer Policy*, 45, p. 561.

2. ELECTRONIC SPORTS REGULATION: A BRIEF OVERVIEW AND KEY STAKEHOLDERS

2.1. DEFINING ESPORTS AND REGULATORY CHALLENGES

ESports have rapidly evolved into a global phenomenon, blurring the lines between traditional sports, entertainment, and digital services. With millions of players and spectators worldwide, competitive gaming has attracted increasing legal and regulatory attention. ESports are generally understood as organised, competitive play of video games at professional or semi-professional levels, governed by structured tournaments, prize pools, and broadcasting ecosystems.²⁰ This narrow definition also limits the scope of the DSA analysis that follows. The article does not examine the regulation of online gaming platforms generally. Examples such as Roblox, Minecraft, or Second Life are relevant as contrast cases showing how gaming-related UGC platforms may differ from eSports infrastructures. The focus remains on professional or semi-professional competitive ecosystems and the services that support them.

Unlike casual or recreational gaming, eSports involve codified rules, rankings, and competitive integrity mechanisms similar to traditional sports. Core esports ss include *League of Legends*, *Counter-Strike 2*, *Dota 2*, *Valorant*, and *Overwatch*. These games feature international players, professional tournaments run by publishers or third parties, prize money and sponsorship as main revenue sources, and a robust streaming and media ecosystem. This distinction excludes games such as *Minecraft*, *Roblox*, or *The Sims*, which may involve user creativity and casual competition but do not contain a professional competitive scene with codified tournament play. Understanding eSports in this narrow, competitive sense is critical when assessing its interaction with EU regulations such as the DSA.

Gábris et al. provided a useful overview of legal challenges surrounding eSports regulation and governance. Three areas of interest shall be particularly mentioned: (i) defining eSports as a legal concept, (ii) governance model for eSports and (iii) legal regulation *per se*.²¹

²⁰ Hamari, J. and Sjöblom, M. (2017) 'What Is eSports and Why Do People Watch It?' *Internet Research*, 27, p. 211; Taylor, T.L. (2012) *Raising the Stakes: E-Sports and the Professionalization of Computer Gaming*. Cambridge, MA: MIT Press; Jenny, S.E., Manning, R.D., Keiper, M.C. and Olrich, T.W. (2017) 'Virtual(ly) Athletes: Where eSports Fit Within the Definition of "Sport"'. *Quest*, 69, p. 1; Tang, D., Kim-wai Sum, R., Li, M., Ma, R., Chung, P. and Ho, R.W.-k. (2023) 'What Is ESports? A Systematic Scoping Review and Concept Analysis of ESports'. *Heliyon*, 9, e23248.

²¹ Gábris, T., Hamul'ák, O., Kocharyan, H. and Martínez Ramil, P. (2024) 'ESports Between the Sports and Entertainment Industry: In Search of Division Lines'. *TalTech Journal of European Studies*, 14(2), p. 190.

The legal classification of eSports remains a subject of debate, with scholars and regulators questioning whether it should be considered a sport, a segment of the entertainment industry, or even a digital form of performing arts. Two opposing perspectives frame this discussion. On one hand, various non-European countries and international sports organizations, including the International Olympic Committee, increasingly recognize eSports as part of the sporting domain.²² On the other hand, some scholars argue that eSports lack the defining characteristics of traditional sports, such as physicality and full-body control, and therefore do not contribute to human physical development in the same way.²³ Additionally, concerns have been raised regarding the commercial nature of eSports, particularly in relation to ownership structures and governance models, which differ significantly from conventional sports institutions.²⁴

Another key issue in eSports regulation is the governance model that best fits its structure. In the context of sports law, two dominant models exist: the European model, which emphasizes a pyramid structure with federations overseeing competition and development, and the North American model, which relies on franchise-based leagues with significant autonomy. Some scholars suggest that the North American model is more applicable to eSports governance, given the industry's reliance on private entities, including game publishers and tournament organizers, rather than centralized governing bodies.²⁵ This model allows for greater flexibility in rule-making and commercial operations while recognizing eSports' unique market-driven characteristics.

Beyond autonomous governance, the increasing commercialization of eSports necessitates external regulatory oversight. As state authorities and international institutions turn their attention to eSports, the balance between industry self-regulation and government-imposed rules becomes a crucial legal issue.²⁶ Several key regulatory challenges have emerged, including gender equality, accessibility for disabled players, protection of minors, cyberbullying, doping (such as Adderall abuse), match-fixing, and

²² Tang, D., Kim-wai Sum, R., Li, M., Ma, R., Chung, P. and Ho, R.W.-k. (2023) 'What Is ESports? A Systematic Scoping Review and Concept Analysis of Esports'. *Heliyon*, 9, e23248. Naraine, M.L. (2021) 'Actually, ESports Is Sport: A Response to Parry's (2019) Misguided View'. *Sports Innovation Journal*, 2, p. 33;

²³ Parry, J. (2018) 'E-sports Are Not Sports'. *Sports, Ethics and Philosophy*, 13, p. 3;

²⁴ Ibid.

²⁵ Hong, H.J. (2023) 'eSports: The Need for a Structured Support System for Players'. *European Sport Management Quarterly*, 23, p. 1430. Marelić, M. and Vukušić, D. (2019) 'E-sports: Definition and Social Implications'. *EQOL Journal*, 11(2), p. 47.

²⁶ Martinelli, J. (2019) 'The Challenges of Implementing a Governing Body for Regulating ESports'. *University of Miami International and Comparative Law Review*, 26, p. 499.

cheating. Addressing these concerns requires both industry-led initiatives and formal legal interventions to ensure fair competition and a safe gaming environment. At present, eSports governance is largely driven by industry organizations such as the International ESports Federation (IESF), the Global ESports Federation, and the ESports Integrity Coalition (ESIC), which operate under the Electronic Sports League (ESL) framework. These bodies establish and enforce industry standards, but their rules must align with national and international legal frameworks to prevent conflicts with binding regulations. As legal scrutiny increases, particularly within the EU, dedicated eSports regulations may emerge to address the sector's specific needs while maintaining consistency with broader digital and consumer protection laws. Academic analyses have already explored the intersection of loot boxes and EU digital legislation in the field of consumer protection and unfair commercial practices.²⁷

2.2.KEY STAKEHOLDERS IN THE ESPORTS INDUSTRY

Esports consist of the ecosystem of various actors with distinct stakeholders including game publishers, tournament organisers, streaming platforms, players, and audiences.²⁸ Each stakeholder plays different role and holds varied legal status under the regulation of digital services as discussed in the following chapter.

Publishers such as Riot Games (*League of Legends*, *Valorant*) and Valve Corporation (*Counter-Strike*, *Dota 2*) control the intellectual-property rights, server infrastructure, matchmaking systems, and anti-cheat mechanisms that underpin competition.²⁹ They also regulate access to official tournaments through licence agreements and patch cycles that can materially affect competitive balance. Scholars describe publishers as “rule-makers and gatekeepers” of eSports industry.³⁰ Independent organisers like ESL Gaming, BLAST Premier, DreamHack or officially affiliated leagues manage

²⁷ Leahy, D. (2022) ‘Rocking the Boat: Loot Boxes in Online Digital Games, the Regulatory Challenge, and the EU’s Unfair Commercial Practices Directive’. *Journal of Consumer Policy*, 45, p. 561.

²⁸ Martinelli, J. (2019) ‘The Challenges of Implementing a Governing Body for Regulating ESports’. *University of Miami International and Comparative Law Review*, 26, p. 499; Hong, H.J. (2023) ‘eSports: The Need for a Structured Support System for Players’. *European Sport Management Quarterly*, 23, p. 1430. Marelić, M. and Vukušić, D. (2019) ‘E-sports: Definition and Social Implications’. *EQOL Journal*, 11(2), p. 47.

²⁹ Taylor, T.L. (2012) *Raising the Stakes: E-Sports and the Professionalization of Computer Gaming*. Cambridge, MA: MIT Press; Holden, J. T., Kaburakis, A. and Rodenberg, R. M. (2017) ‘Esports Corruption: Gambling, Doping, and Global Governance’. *Maryland Journal of International Law*, 32, pp. 236–258. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2831718 [Accessed 27 May 2025].

³⁰ Jenny, S.E., Manning, R.D., Keiper, M.C. and Olrich, T.W. (2017) ‘Virtual(ly) Athletes: Where eSports Fit Within the Definition of “Sport”’. *Quest*, 69, p. 1;

competitive events, participant registration, and disciplinary rules.³¹ Their platforms may store information submitted by participants, teams, spectators, or staff, including registration data, player profiles, complaints, comments, or chat messages. By contrast, brackets, official results, schedules, and editorial commentary generated by the organiser itself shall not automatically be treated as information stored at the request of recipients of the service. They also act as private regulators, enforcing codes of conduct and safeguarding policies. Esports reach global audiences primarily through streaming platforms like Twitch, YouTube Gaming or regional services. These providers host user-generated content and operate interactive chat functions. Professional players and teams are recipients of these digital services, bound by tournament terms and publisher licence agreements.³² Audiences interact through live-chat, discussion forums, and potentially social media extensions, creating vast streams of user-generated content.

As evident from the above discussion and brief sketch of key stakeholders, the classification of these subjects varies due to their different role, tasks and competences in the eSports ecosystem. In the following chapter, more in-depth analysis of how the regulation of digital services is applicable to the phenomenon is presented.

3. EU ACT ON DIGITAL SERVICES AND ELECTRONIC SPORTS

3.1.ELECTRONIC GAMES, ESPORTS AND SCOPE OF THE ACT ON DIGITAL SERVICES

The purpose of the DSA is to ensure the effective functioning of the internal market for intermediary services by introducing harmonized rules that create a secure, predictable, and trustworthy online environment. These rules are designed to encourage innovation while safeguarding fundamental rights established in the Charter of the fundamental rights and freedoms, including the principle of consumer protection. The regulation establishes a uniform legal framework governing the provision of intermediary services within the internal market. It outlines conditions for exemption from liability for intermediary service providers, introduces due diligence obligations tailored to specific categories of providers, and sets out enforcement

³¹ Martinelli, J. (2019) 'The Challenges of Implementing a Governing Body for Regulating ESports'. *University of Miami International and Comparative Law Review*, 26, p. 499; Hong, H.J. (2023) 'eSports: The Need for a Structured Support System for Players'. *European Sport Management Quarterly*, 23, p. 1430

³² Gábriš, T., Hamulák, O., Kocharyan, H. and Martínez Ramil, P. (2024) 'ESports Between the Sports and Entertainment Industry: In Search of Division Lines'. *TalTech Journal of European Studies*, 14(2), p. 197..

mechanisms, including measures to enhance cooperation and coordination among competent authorities.³³ Although electronic games are not directly mentioned in the regulation, it is of the essence to note that the regulation applies to broad range of digital services.

The DSA is built on a graduated and nested taxonomy of services. These include intermediary services, hosting services, online platforms, and very large online platforms (VLOPs). The broadest category, intermediary services, defined as information society service³⁴ is further divided into three types: mere conduit, caching, and hosting services. Mere conduit services, such as internet service providers and public Wi-Fi network operators, facilitate the transmission of data without altering its content. Caching services temporarily store information to enhance performance and efficiency. Hosting services encompass web hosting, cloud storage, social media networks, and online advertising platforms.³⁵

Online platforms form a further subcategory of hosting services. They store information provided by recipients of the service and disseminate that information to the public at the request of those recipients, unless the dissemination function is merely minor and purely ancillary to another service.³⁶

VLOPs are, in turn, a subset of online platforms that meet the statutory threshold and are designated by the Commission.³⁷ The DSA also regulates very large online search engines, although these categories are less central to the eSports ecosystem examined here. Legal scholars, such as Husovec, emphasize that determining whether a service falls within the scope of the DSA requires a detailed, case-by-case assessment.³⁸ In some instances, only specific functions of a platform may be subject to the regulation. Moreover, VLOPs are subject to unique regulatory scrutiny, with the European Commission holding exclusive oversight authority over these entities.³⁹

This is essential for eSports because the same undertaking may operate several legally distinct functions. A publisher may supply official game content, store account information, operate private communication tools, host public UGC repositories, and maintain social or marketplace interfaces.

³³ DSA, Article 1.

³⁴ Services normally provided against remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See DSA, Article 3 (a).

³⁵ Article 3 (g), DSA.

³⁶ Article 3 (i), DSA.

³⁷ Article 33 (4), DSA.

³⁸ Husovec, M. (2024) *Principles of Digital Services Act*. Oxford: Oxford University Press.

³⁹ Article 56 (3), DSA.

These functions should not be classified collectively. The DSA analysis must instead ask, function by function, whether the service stores information provided by a recipient, whether it disseminates that information to the public, and whether the dissemination is sufficiently central rather than minor or purely ancillary.

To determine how electronic sports (and more broadly electronic games) fit within the service categories defined by the DSA requires a functional interpretation grounded in Article 3. The DSA regulates services that “consist of the storage of information provided by, and at the request of, a recipient of the service.”⁴⁰ In doctrinal terms, this corresponds to hosting services. As outlined above, a narrower group online platforms refers to hosting services that also disseminate user-generated content (UGC) to the public.⁴¹

The DSA governs activities of intermediation, not the supply of digital content as such. With that in mind, *standalone* or *offline* games, which simply execute locally on the user’s device, fall outside the scope of the DSA. They are software products, not intermediary environments.

By contrast, networked games with interactive or competitive features including those forming the basis of eSports ecosystems often include elements of intermediation. Publishers operate game servers that store and process player data, match histories, chat messages, or replays. These activities satisfy the functional definition of hosting services, as they involve storage of user information at the user’s request.⁴² Examples include *Counter-Strike 2*, *Dota 2*, and *Valorant*, whose publishers maintain persistent accounts and player statistics on centralised servers.

The European Commission’s Impact Assessment supports this interpretation, noting that the term “information society service” under EU law is to be understood broadly and includes online environments facilitating user interaction.⁴³

⁴⁰ Article 3 (g) (iii), DSA.

⁴¹ Article 3 (i), DSA.

⁴² See in general e.g. Wilman, F., Kalèda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press, p. 73-74.

⁴³ European Commission. (2020) *Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services COM(2020) 825 final SEC(2020) 432 final SWD(2020) 349 final*. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0348> [Accessed 27 May 2025], p. 22.

The decisive factor for further classification as an online platform under Article 3(i) is whether the service publicly disseminates user-generated content. Two cumulative conditions apply:

- The content must reach a potentially unlimited number of recipients and
- Dissemination of UGC must be a core functionality, not ancillary to the service.⁴⁴

Recital 13 DSA further clarifies that features that are “minor and purely ancillary” to a principal service such as a comments section on a newspaper website do not transform the entire service into an online platform. Gaming-related services differ substantially in the degree to which UGC is publicly disseminated. Some environments may be structured around private servers, closed groups, or limited sharing functions. Others, however, are built around public UGC dissemination and may provide clearer examples of functions of online platforms. To illustrate the complexity, Roblox⁴⁵ should be better treated as a contrast case of a gaming-related UGC platform rather than as a peripheral or non-public example. It is not central to this article’s narrow definition of eSports, but it illustrates why gaming services cannot be excluded from the DSA analysis in general.

However, the situation differs in eSports competitive titles. Many competitive games integrate mechanisms for publishing or trading user content that circulates publicly and sometimes commercially like custom skins, maps, and highlight replays. For example, Counter-Strike’s iconic “Dust2” map originated as a user-generated modification, later officially integrated into the game and disseminated to millions of players.⁴⁶ Similarly, publishers like Valve host public marketplaces representing places where players trade skins or mods, creating a clear dissemination function.

The legal character of UGC may also change over time. Where a player uploads a map, skin, mod, replay, or other item and the provider stores and publicly disseminates it at the request of that player, the relevant function may fall within Article 3(i). However, if the provider later selects,

⁴⁴ Wilman, F., Kaléda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press, p. 39-40.

⁴⁵ See e.g. Authority for Consumers and Markets. (2026). *ACM launches investigation into Roblox in connection with risks that minors are facing*. Available from <https://www.acm.nl/en/publications/acm-launches-investigation-roblox-connection-risks-minors-are-facing> [Accessed 1 June 2026].

⁴⁶ Duan, H., Huang, Y., Zhao, Y., Huang, Z. and Cai, W. (2022) ‘User-Generated Content and Editors in Video Games: Survey and Vision’. Available from: <https://faculty.washington.edu/weicaics/paper/papers/HaihanDHZHC2022.pdf> [Accessed 27 May 2025].

edits, integrates, and republishes that content as part of the official game environment, the relationship becomes more complex. At that stage, the content may no longer be disseminated merely at the request of the original recipient, but as part of the provider's own editorial or commercial decision. The DSA analysis should therefore distinguish the initial UGC dissemination phase from subsequent provider adoption. Moreover, the argument that user-generated content is ancillary in gaming contexts overlooks how modern gaming ecosystems are fundamentally intertwined with creativity driven by players themselves. Whether UGC functions are ancillary or central cannot be presumed for gaming services as a class. It depends on the design of the service. A public mod repository, skin marketplace, or map workshop may be central to a platform's economic or community architecture, whereas a limited chat function or cosmetic profile feature may remain ancillary to gameplay. The classification therefore requires a case-by-case assessment of the role played by UGC in the service's overall functionality, visibility, and monetisation.

Nevertheless, challenges remain in operationalizing this classification. Not all electronic games may meet the threshold of public dissemination or centrality of user-generated content. Distinguishing between core and ancillary user-generated functionalities will require careful evaluation.

A distinction must be drawn between the game as digital content controlled by a provider and particular functions concerning storage of information connected to the game. The fact that a competitive title is online, multiplayer, or based on server does not by itself make the game an online platform. The DSA is concerned with intermediation reflecting that the storage, transmission, or dissemination of information are provided by recipients of the service. Accordingly, official game code, maps, balance patches, characters, rules, and content created by publisher should normally be treated as the provider's own digital content rather than as hosted recipient information.

By contrast, information provided by players may bring specific functions within the hosting category. Examples include account profiles, public usernames, chat messages, forum posts, complaints, uploaded replays, player-created maps, skins, mods, or other UGC. These functions may be hosting services where the relevant information is stored at the request of the recipient. They may become functions relevant for classification as online platforms only where that information is also disseminated to the public and the dissemination is not minor or purely ancillary.

3.2. ESPORTS STAKEHOLDERS AND SCOPE OF THE DSA

The functional distinctions drawn above have direct consequences for the different stakeholders operating within the eSports ecosystem. Each actor provides digital services with distinct degrees of intermediation and public dissemination, determining its classification under the DSA.

Publishers perform the most complex set of functions. They host and operate game servers that store player accounts, rankings, and match data representing activities consistent with the DSA definition of hosting services. In many cases, they go further by facilitating UGC and enabling its public dissemination through in-game workshops or trading markets. Valve's Steam Workshop exemplifies this dual role where players upload custom maps and skins that can be shared or sold to a wide audience. The dissemination is not "ancillary" to gameplay but central to the game's economic and creative ecosystem.⁴⁷ Consequently, publishers should not be classified as online platforms merely because they operate competitive online games. They may, however, operate functions relevant for online platforms where they provide public UGC workshops, marketplaces, replay-sharing libraries, community hubs, or comparable interfaces that disseminate recipient-provided information to an unrestricted public. In other cases, publishers may be hosting providers only or may fall outside the intermediary categories for game content controlled by providers.

From a legal perspective, the hybrid nature of these functions means that a single publisher may simultaneously operate both hosting and online platform components. Husovec emphasises that the DSA requires a functional segmentation of services reflecting the idea that classification attaches to features, not to the entity as a whole.⁴⁸

Tournament organisers occupy an intermediary position between publishers, players, teams, and audiences. They may provide registration systems, player dashboards, complaint tools, communication channels, or event portals that store information submitted by recipients of the service. These functions may qualify as hosting services. For classification as online platform it is also required that the organiser must disseminate information provided by the recipient to the public, and that dissemination must not

⁴⁷ Sas, M. (2024) 'Online Games in the Crosshair: Is the DSA Protecting Players? Part 1'. *CITIP Blog*. Available from: <https://www.law.kuleuven.be/citip/blog/online-games-in-the-crosshair-is-the-dsa-protecting-players-part-1/> [Accessed 27 May 2025] and Sas, M. (2024) 'Online Games in the Crosshair: Is the DSA Protecting Players? Part 2'. *CITIP Blog*. Available from: <https://www.law.kuleuven.be/citip/blog/online-games-in-the-crosshair-is-the-dsa-protecting-players-part-2/> [Accessed 27 May 2025].

⁴⁸ Husovec, M. (2024) *Principles of Digital Services Act*. Oxford: Oxford University Press, p. 172-173.

be minor or purely ancillary to the principal tournament service. Public comment sections, fan forums, spectator chats, or user-uploaded media galleries may satisfy this requirement in some cases. By contrast, official schedules, brackets, rankings, match results, editorial commentary, or curated broadcast content generated by the organiser itself should not automatically be treated as public dissemination of UGC.⁴⁹ On present evidence, tournament organisers are unlikely to meet VLOP thresholds in their own right, although their events may be distributed through VLOP or online streaming services.

Streaming and video-sharing platforms form the outer layer of the eSports ecosystem and are the most clearly regulated under the DSA. They host, store, and publicly disseminate audiovisual content and chat messages created by millions of users. These services are online platforms, and YouTube is already formally designated as VLOP.⁵⁰ Their role in eSports extends beyond passive broadcasting. Recommender systems curate which tournaments, teams, or streamers are promoted to users, while real-time chat moderation implicates notice-and-action mechanisms and risk-mitigation obligations. Consequently, streaming platforms bear the most extensive DSA obligations within the eSports chain.

For this reason, the most straightforward DSA implications in eSports arise not from the competitive game itself, but from the broadcasting and audience-interaction layer surrounding it.

Audiences in eSports are active participants including minors. They generate content like public messages, comments, memes, replays, flag harmful material, and are targeted by recommender systems and personalised advertisements. While not service providers, audiences are defined as "recipients of the service" under Art. 3(b) DSA and are granted transparency and due-process rights.

⁴⁹ Martinelli, J. (2019) 'The Challenges of Implementing a Governing Body for Regulating eSports'. *University of Miami International and Comparative Law Review*, 26; Wilman, F., Kaleda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press.

⁵⁰ <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-notes>

Stakeholder	Function	Likely DSA Classification	Qualification
Publisher	Official game content, balance patches, official maps	Outside DSA	Provider's own content
Publisher	Player accounts and profiles	Hosting	If information is stored at the player's request
Publisher	Private or team chat	Hosting	Not necessarily public dissemination
Publisher	Public chat, forums, community hubs	Possible online platform	If public and non-ancillary
Publisher	Public UGC workshop, skin market, mod repository	Possible online platform	Strongest publisher-side case
Publisher	UGC later adopted into official game	Likely provider of content after adoption	Requires lifecycle analysis
Tournament organiser	Registration portal, complaint system, player dashboard	Hosting	Information submitted by recipient
Tournament organiser	Official brackets, schedules, results	Usually not UGC dissemination	Information created by organisers
Tournament organiser	Public fan chat, comment section, media gallery	Possible online platform	Only if non-ancillary
Streaming platform	Streams, clips, comments, live chat	Online platform	Clearest DSA case
Streaming platform	Large-scale eSports content distribution	Possible VLOP	If designated / threshold met
Audience/player/team	Uses services, submits information	Recipient of the service	Not a provider

Table 1: eSports stakeholders and their potential classification according to the DSA

The distinctions summarised in Table 1 also demonstrate the limits of the DSA's relevance to the eSports ecosystem. While streaming services and public UGC infrastructures provide relatively clear examples of online platforms, many activities of publishers and tournament organisers remain outside the DSA or are subject only to its more limited hosting services obligations. This does not necessarily create a regulatory vacuum. Depending on the activity concerned, the relevant legal framework may instead consist of consumer protection law, data protection law, national contract law, or private tournament and integrity rules. The following discussion should therefore be understood as applying only where the relevant functional classification and the corresponding personal scope of a DSA obligation have first been established.

4. ESPORTS AND RELEVANT INSTITUTES OF THE DSA

The obligations examined in this section do not apply uniformly to eSports stakeholders. They depend on the classification of the specific function at issue. Some obligations apply to all intermediary services, others only to hosting services, online platforms, or VLOPs. Accordingly, the following analysis does not assume that publishers, tournament organisers, or streaming services are regulated as whole entities. It asks which obligations attach to particular eSports-related functions once those functions satisfy the DSA's criteria.

4.1. TRANSPARENCY AND TERMS OF SERVICE (ARTICLE 14 DSA)

Article 14 DSA obliges all providers of intermediary services to make their terms and conditions (T&Cs) "clear, easily understandable and publicly available," and to specify how they moderate content, apply restrictions, or use automated tools.⁵¹ In terms of classic online platform the obligation means that they are allowed to delineate what kind of content is not allowed on the platform and what are processes and methods in terms of detection of illegal or undesired content. This means, that the obligation does not apply only to the illegal content but also extend the "platform supervision" over content violating contractual terms. Additionally, for intermediary services intended for minors, providers of digital services are expected to make special efforts to ensure that the explanation of their terms and conditions is clear and easily understandable to younger users.⁵²

In eSports, Article 14 is most relevant where terms govern intermediary functions such as public chats, UGC submissions, account restrictions, community hubs, replay-sharing tools, or tournament portals. It should not be read as converting all game rules, balance decisions, patch notes, or competition formats into requirements posed by the DSA. The key distinction is whether the term concerns restrictions on information provided by recipients of the service or merely defines the provider's own game or competition product.

In eSports context, governance requires publishers to disclose game rules, moderation, and disciplinary processes. However, it shall be born in mind that these provisions are directed only towards information provided by the recipients of service i.e. UGC component. Organisers must provide transparent codes of conduct and event policies, especially regarding chat moderation. Streaming platforms need to provide explanations as well, particularly in case of using AI-based moderation during broadcasts.

⁵¹ Article 14 (1), DSA.

⁵² Recital 46, DSA.

Article 14 introduces a horizontal transparency standard for all intermediaries, shifting EU platform regulation from a reactive liability model to a proactive governance model. In eSports, Article 14 may transform some forms of community management from purely contractual discretion into a regulated transparency domain. This is particularly relevant for public-facing moderation rules, account restrictions linked to user-generated information, and tournament-portal communication policies. In practice, relevant stakeholders shall consider the context of fundamental rights and freedom within the obligation.⁵³

4.2.CONTENT MODERATION PROCEDURES (ARTICLES 16–17 DSA)

Articles 16 and 17 DSA establish notice-and-action procedures for illegal content and require platforms to issue a statement of reasons when restricting content or user access.⁵⁴ In the context of competitive gaming and streaming, content restrictions are frequently enforced. Examples include deleting chat messages containing offensive or defamatory language during live events, removing broadcasts featuring copyrighted music or match footage without proper authorization or temporarily suspending spectators who engage in spamming or hate speech.

A distinctive eSports problem concerns the timing of moderation. Live tournaments and ad hoc event platforms may last only a few hours or days, while moderation decisions may have immediate effects on participation, visibility, or audience interaction. Statements of reasons under Article 17 should therefore be designed for rapid delivery and practical usefulness. A notice issued after the event has ended may formally satisfy a transparency requirement but fail to provide meaningful procedural protection in the context of live competition or real-time broadcasting.

Cheating itself is not normally “illegal content” within the meaning of the DSA. It will usually be treated primarily as a breach of the publisher’s end-user licence agreement, tournament rules, or other contractual integrity standards. Consequently, the detection of prohibited software, disqualification of a player, forfeiture of prize money, or suspension from competition should not automatically be characterised as DSA content moderation. Articles 16 and 17 become relevant only where the conduct involves information stored at the request of a recipient of a hosting service, for example cheating-related uploads, unlawful circumvention tools, doxxing, threats, or public accusations. Article 17 may also apply to defined

⁵³ Quintais, J. (2023) ‘Using Terms and Conditions to Apply Fundamental Rights to Content Moderation’. *German Law Journal*.

⁵⁴ DSA, Article 16 and 17.

restrictions imposed because information provided by recipient is considered illegal or incompatible with the provider's terms and conditions. Outside those situations, procedural safeguards concerning cheating sanctions must be sought primarily in contract law, applicable consumer protection rules, tournament procedures, and private integrity governance.

While platforms shall routinely undertake these actions, the DSA mandates that they provide structured and reasoned notifications to users whose content or accounts are impacted. Additionally, tournament organizers managing online platforms may be further required to establish effective reporting mechanisms for issues such as cheating-related content or doxxing incidents, as these are in general prohibited during competitions.

As literature emphasises, the DSA "constitutionalises platform governance," replacing discretionary enforcement with procedural safeguards.⁵⁵ For eSports, this proceduralising may reduce arbitrariness in moderation decisions that has been a subject to a community tension for a long time.⁵⁶

4.3.PROTECTION OF MINORS

In terms of protecting minors, platforms must take appropriate and proportionate measures to ensure a safe online environment for children and adolescents.⁵⁷ This includes designing interfaces and functionalities that are age-appropriate and limiting the use of profiling-based recommender systems for targeting minors.⁵⁸ This provision is targeted to online platforms accessible to minors. Accessibility may stem from three situations. Firstly, when online platforms are permitted to be used by minors. Secondly, when an online platform is directed at minors. Thirdly, when an online platform is aware that part of the user base is formed by minors.⁵⁹

It shall be emphasized that many electronic games do not have adult only policies and large portion of user base are minors. The obligation to adopt 'appropriate' measures can be understood as requiring online platforms to thoroughly evaluate the potential impact their services may have on the safety and well-being of minors. This involves a comprehensive assessment of all relevant factors and risks associated with the specific

⁵⁵ Frosio, G. and Geiger, C. (2024) 'Towards a Digital Constitution: How the Digital Services Act Shapes the Future of Online Governance'. *VerfBlog*. Available from: <https://verfassungsblog.de/towards-a-digital-constitution/>

⁵⁶ Taylor, T.L. (2012) *Raising the Stakes: E-Sports and the Professionalization of Computer Gaming*. Cambridge, MA: MIT Press;

⁵⁷ DSA, Article 28 (1).

⁵⁸ DSA, Article 28 (2).

⁵⁹ DSA, Recital 71.

nature of the platform's content and functionalities.⁶⁰ What constitutes an appropriate response will therefore vary depending on the type of content being shared and the characteristics of the platform in question. The extent of these measures is guided by the overarching principle of proportionality, a cornerstone of EU law, ensuring that the actions taken are balanced and tailored to the level of risk presented.⁶¹

In the eSports context, Article 28 is most relevant where minors participate in or interact with functions of online platforms connected to competitive gaming. This may include youth tournaments, junior leagues, team recruitment portals, public spectator chats, event fan zones, streaming chats, and eSports advertising or sponsorship interfaces. The provision is less directly relevant to the game as such unless the relevant function qualifies as an online platform accessible to minors.

Platforms may be also encouraged to conduct child rights impact assessments, considering the potential risks their services may pose to young users. The restriction on profiling is triggered only when the provider of the online platform can be reasonably certain that the user whose personal data is being processed is a minor. The notion of "awareness" in this context implies a standard of constructive knowledge, meaning the provider is expected to act on information that reasonably indicates the user's age, even if they do not have direct confirmation.⁶²

The European Commission has recently introduced guidelines for protection of minors according to the DSA.⁶³ The Guidelines emphasize measures against AI-enhanced nudging in the context of electronic games, in-game purchases resembling dark patterns, offering micro-transactions during critical moments in the game and protection of minors as consumers while gaming.⁶⁴

⁶⁰ By analogy, scholarship on child-centric gaming platforms such as Roblox illustrates how Article 28 may require context-sensitive assessment of safety and well-being risks for minors. Chawki, M. (2025) 'AI Moderation and Legal Frameworks in Child-Centric Social Media: A Case Study of Roblox'. *Laws*, 14, p. 29. Available from: <https://doi.org/10.3390/laws14030029> [Accessed 27 May 2025]

⁶¹ Wilman, F., Kalėda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press.

⁶² *Ibid.*

⁶³ European Commission. (2025) *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(1) of Regulation (EU) 2022/2065, C/2025/5519*.

⁶⁴ *Ibid.*

The protection of minors is essential in the eSports environment, where the user base includes a large number of under-18 participants and spectators.⁶⁵

Where a function qualifies as an online platform accessible to minors, the publisher may need to consider age-appropriate defaults and safety settings for that function, such as public chat, community hubs, or UGC-sharing spaces. These may include in-game chat restrictions, content filters, and spending limits configured to protect younger users. Parental control dashboards that have been long recognised in the industry as effective voluntary safeguards⁶⁶ may also contribute to DSA compliance by demonstrating proactive measure mitigating risks. The challenge lies in balancing such measures with commercial features like personalised offers or microtransactions, which may constitute manipulative nudging contrary to Article 25 DSA.

Organisers of eSports events are encouraged to adopt codes of conduct and safeguarding procedures for youth participants. Guidance from the eSports Integrity Commission⁶⁷ and UNICEF⁶⁸ identify specific risks including unsupervised communication, coaching abuse, and exposure to gambling promotion. In line with Article 28, organisers should implement background-check policies, monitor communication channels to detect abusive behaviour, and accessible reporting systems for minors, paralleling existing sport-integrity frameworks.

For tournament organisers, the more eSports-specific issue is not merely exposure to harmful online content, but the overlap between platform governance and safeguarding including coach-player communication, team recruitment, youth tournaments, reporting of abuse, and sponsorship or gambling-adjacent messaging around events.

Performing child-rights impact assessments and limiting profiling-based recommender systems for minors⁶⁹ may be unnecessary measures taken by

⁶⁵ UNICEF. (2020) *Online gaming: respecting and supporting children's rights and well-being*. Available from: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming> [Accessed 27 May 2025].

⁶⁶ Entertainment Software Rating Board. (2007) *Parents increasingly using ESRB ratings to restrict the video games their children play*. Available from: <https://www.esrb.org/blog/parents-increasingly-using-esrb-ratings-to-restrict-the-video-games-their-children-play/> [Accessed 27 May 2025].

⁶⁷ eSports Integrity Commission. (2019) *The Importance of Child Protection in eSports*. Available from: <https://esic.gg/industry-update/the-importance-of-child-protection-in-esports/> [Accessed 27 May 2025].

⁶⁸ UNICEF. (2020) *Online gaming: respecting and supporting children's rights and well-being*. Available from: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming> [Accessed 27 May 2025].

⁶⁹ European Commission. (2025) 'Commission Publishes Draft Guidelines on Protection of Minors Online under the Digital Services Act'. Available from: <https://digital-st>

streaming platforms. These are also obliged to ensure that advertising and monetisation tools are not targeted at or exploitative of minors, echoing obligation in the Article 28 (2). Their compliance thus connects child protection with duties related to analysis and mitigation of systemic risks under Articles 34 and 35.

The limited personal scope of Article 28 DSA does not mean that minors are left without legal protection where a publisher or tournament service does not qualify as an online platform. Where personal data of minors are processed, the GDPR applies independently of the service's classification under the DSA. Relevant requirements include lawful, fair, and transparent processing, information presented in language understandable to children, data protection by design and by default, and the special conditions applicable when consent is relied upon for information society services offered directly to children. Minors may also constitute a particularly vulnerable group of consumers under Article 5(3) of the Unfair Commercial Practices Directive. Commercial practices involving purchases, virtual currencies, personalised offers, sponsorship, or other monetisation should therefore also be assessed under consumer protection law. The DSA represents one part of a broader protective framework rather than an exhaustive regime for minors participating in eSports.

4.4.PROTECTION OF DESIGN

Design requirements imposed by the DSA focus on preventing manipulative practices known as "dark patterns" that could mislead or exploit users, especially vulnerable groups such as minors.⁷⁰ Platforms must ensure that their interfaces are not deceptive and that users are empowered to make informed choices, for example, when managing privacy settings or consenting to terms of service. An online interface is defined in the DSA as "any software, including a website or a part thereof, and applications, including mobile applications."⁷¹

Further relevant delineations in terms of definitions are provided by the European Data Protection Board in its guidelines on dark patterns and data protection issues. Within the scope of these Guidelines, "deceptive design patterns" refer to user interfaces and navigation paths on social media platforms that are intentionally crafted to steer users toward decisions that they may not intend or wish to make, often resulting in outcomes that

rategy.ec.europa.eu/en/news/commission-publishes-draft-guidelines-protection-minors-online-under-digital-services-act [Accessed 27 May 2025], section 22.

⁷⁰ DSA, Article 25 (1).

⁷¹ DSA, Article 3, point m).

favour the interests of the platforms over those of the users, particularly concerning their personal data. These design patterns exploit cognitive biases, undermining users' ability to effectively manage their personal data and to make well-informed choices. In some cases, they may even prevent users from providing meaningful and voluntary consent. Such manipulation can occur through various design elements, including the use of colours or the strategic placement of content. On the other hand, prioritizing user-centric, transparent, and accessible design can help support compliance with data protection rules.⁷² Although social media environment is primary subject of guidelines, video games are explicitly mentioned as relevant area for assessing dark patterns.⁷³

However, the applicability of discussed provisions is limited to situations, where other EU law does not apply. This is the case of unfair commercial practices and data protection laws.⁷⁴ Such limit triggered a discussion on the role of the Article 25 in the wider EU legal framework. As Husovec points out, the application of provisions is still valid in case of business-to-business relations and business-to-consumer requirements stemming directly from the DSA.⁷⁵ Further research shows that these provisions play only complementary role in the "dark pattern" ecosystem.⁷⁶

Article 25 should not be interpreted as imposing a general DSA duty of fair game design or competitive balance. Its relevance is narrower as it concerns the design, organisation, and operation of online interfaces in ways that deceive, manipulate, or materially distort recipients' ability to make free and informed decisions. In eSports relevant services, Article 25 is most relevant to interfaces for purchases, subscriptions, paid visibility, ticketing, sponsorship engagement, account settings, privacy choices, and participation prompts. Where such interfaces belong to an online platform, design features such as misleading countdowns, hidden costs, repeated purchase prompts, or paid engagement tools may raise DSA concerns. By contrast, balance patches, character abilities, weapon statistics, or the internal design of competitive gameplay should not be treated as Article 25 issues merely because they

⁷² European Data Protection Board. (2022) *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them*. Available from: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en [Accessed 27 May 2025].

⁷³ Ibid.

⁷⁴ DSA, Article 25 (3).

⁷⁵ Husovec, M. (2024) *Principles of Digital Services Act*. Oxford: Oxford University Press

⁷⁶ Esposito, F. and Maciel Cathoud Ferreira, T. (2024) 'Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns'. *European Journal of Risk Regulation*, 15.

affect competitive integrity. Given the emphasis on skill-based fairness in eSports, practices encouraging microtransactions that may affect gameplay performance could be at odds with Article 25 DSA and the fairness principle outlined in Recital 67. It shall be noted that certain design approaches may influence the validity of user consent regarding data processing or monetisation, linking Article 25 to GDPR transparency requirements.

Organisers are increasingly responsible for user interfaces in competition portals, ticketing, and sponsorship engagement tools. They must ensure that countdown timers, in-event advertising, or bonus participation prompts are not misleading or exploitative. Interface design that induces impulsive spending during live events including paid chat boosts or in-match purchases risks violating the DSA's anti-manipulation standard. Transparent communication of any paid advantages preserves both consumer autonomy and competitive integrity.

Streaming platforms must review how user interacts within broadcasts ranging from subscription prompts, donation pop-ups, to algorithmic "boost" offers with aim to ensure they do not exploit behavioural biases.

This complementary relationship is particularly important where the relevant gaming or tournament interface does not qualify as an online platform pursuant to the DSA. In such circumstances, manipulative purchase prompts, addictive design, unfair personalisation, or misleading presentation of virtual currencies may still be examined under the GDPR and existing consumer protection law. The proposed Digital Fairness Act may provide a more appropriate vehicle for addressing any remaining deficiencies because it is intended to address dark patterns, addictive design, unfair personalisation, and problematic digital contracts beyond the DSA's requirements. Accordingly, the limited applicability of Article 25 to many eSports functions does not, by itself, justify extending the DSA beyond its functional regulatory purpose.

4.5. TRANSPARENCY OF RECOMMENDER SYSTEMS

Transparency of recommender systems is another key aspect. Online platforms must provide clear information about how these systems operate, including the main parameters used to determine what content is shown to users.⁷⁷ This information shall be provided in terms and conditions in clear and plain language.

According to the DSA, recommender systems are defined as "fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise

⁷⁷ DSA, Article 27 (1) and (2).

that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed.”⁷⁸

Users should be informed about whether content is personalized based on profiling or behavioural data and must be given options to modify or opt out of such personalization, where technically feasible.⁷⁹

In eSports, recommender systems influence not only what users see, but also how they compete, train, and interact.

Article 27 is most clearly relevant to eSports where an online platform recommends, ranks, or prioritises eSports-related information in its interface. This includes recommended streams, tournament broadcasts, clips, highlights, teams, creators, fan communities, or event pages. The legal issue is not whether an algorithm assists player performance, but whether an online platform uses a fully or partially automated system to suggest or prioritise specific information to recipients of the service. Publishers must therefore inform users of key ranking parameters (e.g. skill level, purchase history) and disclose whether profiling or behavioural data influence these suggestions.⁸⁰

For publishers, Article 27 will apply only where the relevant function is itself an online platform and uses a recommender system to prioritise information shown to recipients. Only in such circumstances must the provider disclose the main parameters governing the recommender system. Matchmaking, competitive rankings, coaching tools, or loadout recommendations should not be treated as Article 27 recommender systems merely because they employ automated processes.

Tournament organisers may use automated systems to suggest matches, event pages, streams, or other information to users. Article 27 applies, however, only where the organiser operates an online platform and the system recommends or prioritises information within that function. Internal competitive placement, tournament seeding, or recommendations of training modules should not automatically be brought within Article 27.

For streaming platforms, recommender systems determine the visibility of tournaments, teams, and streamers. Where a streaming service qualifies as an online platform and uses a recommender system, Article 27 requires it to explain in its terms and conditions, in clear and intelligible language, the main parameters used by that system and any options available to

⁷⁸ DSA, Article 3, point s).

⁷⁹ DSA, Article 27 (3).

⁸⁰ Wilman, F., Kaleda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press, p. 215.

recipients to modify or influence those parameters. Where several options are available, recipients must be able to select or modify their preferred option.⁸¹ A separate and more demanding obligation applies under Article 38 to VLOPs and VLOSEs, which must provide at least one option that is not based on profiling. Neither Article 27 nor Article 38 necessarily requires a chronological or “neutral” feed. In the eSports context, recommender systems may nevertheless affect competitive visibility by disproportionately benefiting popular teams, creators, or sponsored events.

This is one of the most practically significant DSA issues for eSports, because algorithmic visibility may affect which competitions, teams, and creators reach audiences. The issue is therefore not competitive balance inside the game, but visibility and discoverability in the surrounding content ecosystem.

4.6.PRIVATE GOVERNANCE

A further eSports-specific issue concerns the relationship between the DSA and private integrity governance. eSports is already governed by publisher terms, tournament rulebooks, anti-cheat systems, and bodies such as the ESports Integrity Commission. The DSA does not replace these systems. However, where disciplinary or integrity measures are implemented through intermediary or online-platform functions, DSA duties may affect the procedural environment in which private governance operates.

For example, removal of user-generated accusations, doxxing, threats, or unlawful cheating-related materials may trigger notice-and-action duties. Restrictions on accounts or content connected to public platform functions may require statements of reasons. Terms governing public communication channels may need to be sufficiently clear under Article 14. The practical consequence is that eSports integrity governance cannot be analysed only as private ordering, rather in some contexts, it becomes embedded in regulated platform infrastructure.

As discussed above, DSA representing the regulation of digital services in general possess the potential to influence electronic games including eSports competitive titles. Below is the table summarising potential duties and requirements based on different stakeholders playing a role in eSports.

⁸¹ Busch, C. (2023) ‘From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation’. In: Milano, S. and Taddeo, M. (eds) *Recommender Systems: Legal and Ethical Issues*. Cham: Springer, pp. 31–54. Available from: https://doi.org/10.1007/978-3-031-34804-4_3 [Accessed 29 June 2026].

Function	Relevant DSA obligations	eSports specific issue
Public live chat on streaming platform	Articles 14, 16, 17; possibly 28, 34, 35 for VLOPs	Real-time moderation, hate speech, doxxing, event timing
Tournament portal with data submitted by participants	Article 14; Articles 16–17 if hosting illegal content reports	Clarity of rules, complaints, account restrictions
Public comment section	Articles 14, 16, 17; possibly online platform duties if non-ancillary	Whether fan interaction is ancillary
Public UGC workshop Skin or mod marketplace	Articles 14, 16, 17; possibly 25, 27, 28	UGC dissemination, monetisation, minors
Official brackets Schedules Match results	Usually outside UGC-based platform duties	Content created by providers
Streaming recommendations for tournaments or creators	Article 27; VLOP duties where applicable	Visibility of teams, events, streamers
Interface for paid boosts, ticketing, subscriptions, donations	Article 25 where operated by online platform	Dark patterns and monetised engagement
Youth tournament communication channels	Article 28 if online platform accessible to minors	Safeguarding, reporting, age-appropriate design
Cheating disputes under tournament rules	Usually outside Articles 16–17 unless illegal content involved	Private governance versus DSA moderation

Table 2: eSports stakeholders and their potential classification according to the DSA.

5. CONCLUSIONS AND FUTURE CHALLENGES

The analysis shows that the DSA does not regulate eSports as such. Its relevance lies in its application to specific intermediary functions within the eSports ecosystem. Competitive games, tournament infrastructures, UGC tools, fan interaction spaces, and streaming environments should therefore not be classified at the level of the actor or sector, but at the level of the relevant service function.

Streaming platforms and public UGC infrastructures provide the clearest cases of online platform regulation. Publishers may operate hosting or online platform functions where they store and publicly disseminate information provided by recipients, but official game content, gameplay mechanics, balance decisions, and content adopted by provider should not automatically fall within that logic. Tournament organisers may be hosting providers in relation to registration portals, participant dashboards, or complaint systems, but publicly available fan tools or chats require a separate ancillary-function analysis. In line with critical commentary on the DSA's expansion of

platform accountability, the findings demonstrate that eSports governance is undergoing a comparable transformation. Transparency of terms, structured notice-and-action processes, and recommender-system disclosures introduce formal procedure to spaces long criticised for opaque moderation and discretionary enforcement. The debates surrounding manipulative design and the protection of minors further demonstrate that the DSA forms only one part of a broader EU regulatory framework. Where the relevant service does not qualify as an online platform, comparable risks may nevertheless fall within consumer protection law or the GDPR. This aligns with emerging work arguing that the regulation increasingly intersects with behavioural design, nudging, and interactive architecture. For eSports, where minors represent a large share of participants and where monetisation models often rely on persuasive interfaces, these duties raise substantial compliance and design questions.

The eSports ecosystem therefore illustrates both the reach and the limits of the DSA. It shows how DSA obligations may enter competitive gaming indirectly through public chats, UGC repositories, streaming platforms, tournament portals, recommender systems, and interfaces accessible to minors. At the same time, it cautions against treating all online games, all tournament activity, or all game-design choices as regulated services or conduct.

The limits identified in this article do not support a general extension of the DSA to every digital function within the eSports ecosystem. In many cases, exclusion from the DSA reflects a deliberate allocation between different regulatory regimes rather than an unintended legal gap. Processing of player data remains governed by the GDPR; commercial practices and standard consumer terms remain subject to consumer protection law; and cheating, disciplinary sanctions, and tournament participation are governed primarily by contractual and private integrity frameworks. A more genuine regulatory concern may arise in relation to addictive design, opaque virtual currencies, unfair personalisation, and exploitative practices affecting minors where these occur outside an online-platform function. Such concerns appear more suitable for consideration under the proposed Digital Fairness Act than through an expansion of the DSA's taxonomy.

LIST OF REFERENCES

- [1] Busch, C. (2023) 'From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation'. In: Milano, S. and Taddeo, M. (eds) *Recommender Systems: Legal and Ethical Issues*. Cham: Springer, pp. 31–54. Available from: https://doi.org/10.1007/978-3-031-34804-4_3 [Accessed 29 June 2026].
- [2] Chawki, M. (2025) 'AI Moderation and Legal Frameworks in Child-Centric Social Media: A Case Study of Roblox'. *Laws*, 14, p. 29. Available from: <https://doi.org/10.3390/laws14030029> [Accessed 27 May 2025].
- [3] Duan, H., Huang, Y., Zhao, Y., Huang, Z. and Cai, W. (2022) 'User-Generated Content and Editors in Video Games: Survey and Vision'. Available from: <https://faculty.washington.edu/weicaics/paper/papers/HaihanD HZHC2022.pdf> [Accessed 27 May 2025].
- [4] Entertainment Software Rating Board. (2007) *Parents increasingly using ESRB ratings to restrict the video games their children play*. Available from: <https://www.esrb.org/blog/parents-increasingly-using-esrb-ratings-to-restrict-the-video-games-their-children-play/> [Accessed 27 May 2025].
- [5] ESports Integrity Commission. (2019) *The Importance of Child Protection in eSports*. Available from: <https://esic.gg/industry-update/the-importance-of-child-protection-in-eSports/> [Accessed 27 May 2025].
- [6] Esposito, F. and Maciel Cathoud Ferreira, T. (2024) 'Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns'. *European Journal of Risk Regulation*, 15, p. 999.
- [7] European Commission. (2020) *Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services COM(2020) 825 final SEC(2020) 432 final SWD(2020) 349 final*. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0348> [Accessed 27 May 2025].
- [8] European Commission. (2025) 'Commission Publishes Draft Guidelines on Protection of Minors Online under the Digital Services Act'. Available from: <https://digital-strategy.ec.europa.eu/en/news/commission-publishes-draft-guidelines-protection-minors-online-under-digital-services-act> [Accessed 27 May 2025].
- [9] European Data Protection Board. (2022) *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them*.

- Available from: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en [Accessed 27 May 2025].
- [10] European Parliament. (2022) *Resolution on the Role of Video Games in the European Economy: Challenges and Opportunities*. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022IP0388> [Accessed 27 May 2025].
- [11] Frosio, G. and Geiger, C. (2024) 'Towards a Digital Constitution: How the Digital Services Act Shapes the Future of Online Governance'. *VerfBlog*. Available from: <https://verfassungsblog.de/towards-a-digital-constitution/>
- [12] Gábriš, T., Hamulák, O., Kocharyan, H. and Martínez Ramil, P. (2024) 'ESports Between the Sports and Entertainment Industry: In Search of Division Lines'. *TalTech Journal of European Studies*, 14(2), p. 190.
- [13] Hamari, J. and Sjöblom, M. (2017) 'What Is eSports and Why Do People Watch It?' *Internet Research*, 27, p. 211.
- [14] Holden, J. T., Kaburakis, A. and Rodenberg, R. M. (2017) 'Esports Corruption: Gambling, Doping, and Global Governance'. *Maryland Journal of International Law*, 32, pp. 236–258. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2831718 [Accessed 27 May 2025].
- [15] Hong, H.J. (2023) 'eSports: The Need for a Structured Support System for Players'. *European Sport Management Quarterly*, 23, p. 1430.
- [16] Husovec, M. (2024) *Principles of Digital Services Act*. Oxford: Oxford University Press.
- [17] Jenny, S.E., Manning, R.D., Keiper, M.C. and Olrich, T.W. (2017) 'Virtual(ly) Athletes: Where eSports Fit Within the Definition of "Sport"'. *Quest*, 69, p. 1.
- [18] Keller, D. (2022) 'The DSA's Industrial Model for Content Moderation'. *Verfassungsblog*, 24 February. Available from: <https://verfassungsblog.de/dsa-industrial-model/> [Accessed 29 June 2026].
- [19] Kusters, L. and Gstrein, O. J. (2023) 'TikTok and Transparency Obligations in the EU Digital Services Act (DSA) – A Scoping Review'. *Zeitschrift für Europarechtliche Studien (ZEuS)*, 01/2024, pp. 110–132. Available from: <https://ssrn.com/abstract=4652543> or <http://dx.doi.org/10.2139/ssrn.4652543> [Accessed 2 December 2023].
- [20] Leahy, D. (2022) 'Rocking the Boat: Loot Boxes in Online Digital Games, the Regulatory Challenge, and the EU's Unfair Commercial Practices Directive'. *Journal of Consumer Policy*, 45, p. 561.

- [21] Luguri, B. and Strahilevitz, L. (2021) 'Shining a Light on Dark Patterns'. *Journal of Legal Analysis*.
- [22] Marelić, M. and Vukušić, D. (2019) 'E-sports: Definition and Social Implications'. *EQOL Journal*, 11(2), p. 47.
- [23] Martinelli, J. (2019) 'The Challenges of Implementing a Governing Body for Regulating ESports'. *University of Miami International and Comparative Law Review*, 26, p. 499.
- [24] MordorIntelligence. (2023) *eSports Market*. Available from: <https://www.mordorintelligence.com/industry-reports/eSports-market> [Accessed 27 May 2025].
- [25] Naraine, M.L. (2021) 'Actually, ESports Is Sport: A Response to Parry's (2019) Misguided View'. *Sports Innovation Journal*, 2, p. 33.
- [26] Naudts, L., Helberger, N., Sax, M. and Veale, M. (2024) 'Toward Constructive Optimisation: A New Perspective on the Regulation of Recommender Systems and the Rights of Users and Society'. In: Helberger, N., Kas, B., Micklitz, H.-W., Namysłowska, M., Naudts, L., Rott, P. and Veale, M. (eds) *Digital Fairness for Consumers*. Brussels: BEUC – The European Consumer Organisation, pp. 25–68. Available from: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf [Accessed 29 June 2026].
- [27] OECD. (2022) *Dark Commercial Patterns*. OECD Digital Economy Papers, No. 336. Paris: OECD Publishing. Available from: <https://doi.org/10.1787/44f5e846-en> [Accessed 29 June 2026].
- [28] Parry, J. (2019) 'E-sports Are Not Sports'. *Sport, Ethics and Philosophy*, 13(1), pp. 3–18. Available from: <https://doi.org/10.1080/17511321.2018.1489419> [Accessed 29 June 2026].
- [29] PwC. (2023) *Future of eSports*. Available from: <https://www.strategyand.pwc.com/ml/en/strategic-foresight/sector-strategies/media/future-of-eSports.html> [Accessed 27 May 2025].
- [30] Quintais, J.P., Appelman, N. and Ó Fathaigh, R. (2023) 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation'. *German Law Journal*, 24(5), pp. 881–911. Available from: <https://www.cambridge.org/core/journals/german-law-journal/article/using-terms-and-conditions-to-apply-fundamental-rights-to-content-moderation/B30B9043D1C6F14AE9C3647A845E6E10> [Accessed 29 June 2026].
- [31] Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A. and Sánchez Chamorro, L. (2024) 'Who is vulnerable to deceptive design patterns? A

- transdisciplinary perspective on the multi-dimensional nature of digital vulnerability'. *Computer Law & Security Review*, 55, 106031. Available from: <https://www.sciencedirect.com/science/article/pii/S0267364924000979?via%3Dihub> [Accessed 27 May 2025].
- [32] Sas, M. (2024) 'Online Games in the Crosshair: Is the DSA Protecting Players? Part 1'. *CITIP Blog*. Available from: <https://www.law.kuleuven.be/citip/blog/online-games-in-the-crosshair-is-the-dsa-protecting-players-part-1/> [Accessed 27 May 2025].
- [33] Sas, M. (2024) 'Online Games in the Crosshair: Is the DSA Protecting Players? Part 2'. *CITIP Blog*. Available from: <https://www.law.kuleuven.be/citip/blog/online-games-in-the-crosshair-is-the-dsa-protecting-players-part-2/> [Accessed 27 May 2025].
- [34] Sifa, R. et al. (2018) 'Behavioural Modelling for Recommender Systems in Digital Games'. *IEEE Transactions on Games*, 3(2), p. 91.
- [35] Sifa, R., Zhai, K., Pawlakos, E. et al. (2018) 'Controlling the Crucible: A Novel PvP Recommender Systems Framework for Destiny'. In: *Proceedings of Australian Computer Science Week, Interactive Entertainment*. ACM.
- [36] Tang, D., Kim-wai Sum, R., Li, M., Ma, R., Chung, P. and Ho, R.W.-k. (2023) 'What Is ESports? A Systematic Scoping Review and Concept Analysis of ESports'. *Heliyon*, 9, e23248.
- [37] Taylor, T.L. (2012) *Raising the Stakes: E-Sports and the Professionalization of Computer Gaming*. Cambridge, MA: MIT Press.
- [38] UNICEF. (2020) *Online gaming: respecting and supporting children's rights and well-being*. Available from: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming> [Accessed 27 May 2025].
- [39] Wilman, F., Kalèda, S.L. and Loewenthal, P.J. (eds) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press.
- [40] Wolters, P. and Gellert, R. (2023) 'Towards a Better Notice-and-Action Mechanism in the DSA'. *JIPITEC*, 14, p. 403.

DOI 10.5817/MUJLT2026-43027

DATA PROTECTION AND CYBERSECURITY GOVERNANCE FOR EVTOL SYSTEMS IN THE UAE: COMPARATIVE LESSONS FROM THE EU AND US

by

SUMAIYA FIROZ NOMANI * MOHAMMAD RABABA [†]
 HUSSAIN AL-AHMAD [‡] HUSAMELDIN MUKHTAR [§]
 NASIRUDEEN MUHAMMAD [¶] SAAD ALI AMIN ^{||}
 BURKHARD SCHAFFER **

The article investigates the data governance challenges arising from the integration of electric vertical take-off and landing (eVTOL) systems into the United Arab Emirates' emerging urban air mobility ecosystem. As eVTOL operations rely on continuous streams of biometric, geolocation and operational telemetry data, existing legal instruments, particularly the UAE Personal Data Protection Law (Federal Decree by Law No. (45) of 2021), national cybersecurity strategies and General Civil Aviation Authority (GCAA) advisories, remain underprepared to regulate these high-risk data flows. The article examines the extent to which UAE

* Sumaiya Firoz Nomani; University of Dubai: College of Law; Research Assistant and Teaching Faculty; E-mail: snomani@ud.ac.ae; ORCID: 0009-0000-8230-5630.

[†] Mohammad Rababa Ph.D.; Ministry of Higher Education and Scientific Research, UAE; Higher Education Expert; ORCID: 0000-0002-2662-8395.

[‡] Hussain Al-Ahmad Ph.D.; University of Dubai, Vice President of Academic Affairs; ORCID: 0000-0002-5781-5476.

[§] Husameldin Mukhtar Ph.D.; University of Dubai, Director of Research; ORCID: 0000-0002-6340-4710.

[¶] Nasiruddeen Muhammad Ph.D.; Abu Dhabi University, Assistant Professor; ORCID: 0000-0002-2314-6358.

^{||} Saad Ali Amin Ph.D.; University of Dubai; ORCID: 0000-0003-4118-8970.

** Burkhard Schaffer; The University of Edinburgh, School of Law; Professor; ORCID: 0000-0002-6025-4593.

frameworks can accommodate the unique risks posed by autonomous, data-driven aviation, including the processing of sensitive passenger data, real-time cross-border transfers, AI-based navigation decisions and the vulnerability of interconnected systems to cyberattacks. Through a doctrinal analysis, it draws comparative insights from the European Union's integrated data protection and aviation cybersecurity model and the United States' decentralised, innovation-led approach. The article argues that aviation-specific data governance standards, enhancing algorithmic accountability and strengthening cybersecurity obligations are essential steps for aligning technological ambition with public safety. It concludes that a coherent, forward-looking regulatory model will be critical for ensuring trust, accountability and operational resilience as the UAE advances its eVTOL deployment plans.

KEY WORDS

data protection, flying taxis, eVTOL, cybersecurity, aviation law, urban air mobility, algorithmic accountability

1. INTRODUCTION

Electric vertical take-off and landing aircraft (eVTOLs) have emerged as an essential part of urban air mobility (UAM). This has caused an unprecedented shift in the global transportation industry.¹ By offering efficient and environmentally friendly transportation options that are also traffic congestion-free, eVTOLs, which are built to function in densely populated urban settings, have the potential to completely revolutionise mobility.² A new set of legal and policy challenges has arisen from the technologies that facilitate eVTOL operations, such as artificial intelligence (AI), autonomous systems, and networked communications, as governments and corporate organisations strive to integrate eVTOLs into urban mobility.³ Concerns regarding cybersecurity and data privacy are perhaps the most significant, as they are essential to public confidence in this emerging industry.

¹ Lim Kin Yip. (2024) *Comprehensive Multi-Disciplinary Design of an Electric Vertical Take-off and Landing Aircraft*. PhD Thesis, Nanyang Technical University, Singapore, 1, 23; Adam P. Cohen, Susan A. Shaheen & Emily M. Farrar (2021) *Urban Air Mobility: History, Ecosystem, Market Potential, and Challenges*. 22 IEEE Transactions on Intelligent Transportation Systems 6074.

² Muhammad Yasir Arafat & Sungbum Pan. (2024) *Urban Air Mobility Communications and Networking: Recent Advances, Techniques, and Challenges* 8 Drones 1; Saba Al-Rubaye, Antonios Tsourdos & Kamesh Namuduri. (2023) *Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle* 7 Drones 1, 2.

³ Senwei Xiang & others. (2024) *Autonomous eVTOL: A summary of researches and challenges* 3 Green Energy and Intelligent Transportation 1, 13.

Data is the foundation of eVTOL ecosystems.⁴ Both the real-time transmission of statistics for air traffic control and the collection of passenger biometric identifiers and geolocation data depend on enormous data flows across various organisations and governments.⁵ There are significant concerns regarding data ownership, consent, cross-border transfer, and the ability of cybersecurity systems to survive malicious attacks or breaches triggered by these factors.⁶ These concerns are especially significant for the United Arab Emirates (UAE) because it is at the forefront of smart city development and technological innovation. Despite Dubai's ambitious plans to introduce eVTOLs as early as 2026,⁷ the regulatory frameworks governing data privacy and aviation cybersecurity in an innovation as novel as eVTOLs, are still being developed.⁸ Yet, the laws governing these data flows are incomplete. The UAE's Personal Data Protection Law and National Cybersecurity Strategy establish general principles but do not offer aviation-specific rules for telemetry, biometric or cross-border data generated by eVTOL operations. Existing General Civil Aviation Authority (GCAA) advisories also do not address data protection or cybersecurity obligations in this context. International frameworks such as the GDPR (General Data Protection Regulation) provide partial guidance but were not designed for high-tech, AI-enabled air mobility. This creates a regulatory gap: operators lack certainty on compliance, liability allocation and safeguards against data misuse or cyberattacks.

This article argues that conventional data protection frameworks, which are designed for transactional data processing, are structurally inadequate for continuous, safety-critical autonomous systems such as eVTOLs. This article explores the data protection challenges posed by eVTOL operations from a UAE perspective. It examines the adequacy of the UAE's Personal

⁴ Saba Al-Rubaye, Antonios Tsourdos & Kamesh Namuduri. (2023) *Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle*. 7 Drones 1, 2.

⁵ Nimra Khan & Marina Efthymiou. (2021) *The use of biometric technology at airports: The case of customs and border protection (CBP)*. 1 International Journal of Information Management Data Insights.

⁶ Alex Matthew. (2024) *Cloud Data Sovereignty Governance and Risk Implications of Cross-Border Cloud Storage*. Available from: <https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage> [Accessed 26 August 2025].

⁷ Abdelhadi Ramahi, Amr Alfiky and Luke Tyson. (2025) *Dubai aims to beat the traffic with 2026 Joby air taxi liftoff* Available from: <https://www.reuters.com/world/middle-east/dubai-aims-beat-traffic-with-2026-joby-air-taxi-liftoff-2025-07-01/> [Accessed 26 August 2025].

⁸ Karim Tolba, 'UAE GCAA unveils National Civil Aviation Cybersecurity Guidelines' (Aviation Business ME, 2 October 2024) <https://www.aviationbusinessme.com/news/gcaa-national-civil-aviation-cybersecurity-guidelines> accessed 26 August 2025.

Data Protection Law (Federal Decree by Law No. (45) of 2021) and associated cybersecurity regulations in addressing the unique risks of urban air mobility systems, particularly the processing of passenger biometrics, continuous geolocation tracking, real-time operational telemetry, cross-border data transfers and heightened exposure to cyberattacks. By combining these perspectives, the technical risks inherent in eVTOL data flows and the legal gaps in the UAE's current data protection and aviation cybersecurity framework, the article identifies key weaknesses, including the absence of aviation-specific data governance rules, limited guidance on biometric and geolocation processing and the lack of mandatory cybersecurity standards for eVTOL operators. These shortcomings frame the core research problem of the article: whether the UAE's emerging regulatory architecture can adequately address the data protection and cybersecurity risks inherent in eVTOL operations. The article proposes legal and policy recommendations to further strengthen the UAE's regulatory architecture, ensuring that the technological innovation of eVTOLs is aligned with effective data protection and public safety rules and regulations. Although the article focuses on eVTOL operations, many of the underlying cybersecurity and privacy risks arise across autonomous aviation, however, the distinct concern in the context of eVTOLs lies in their convergence with passenger carrying operations, dense urban deployment and continuous processing of data linked to passengers.

2. UNDERSTANDING EVTOL TECHNOLOGY AND DATA

The advent of eVTOLs marks a substantial shift from traditional aviation models, not only in terms of infrastructure or propulsion but more importantly in the type of technologies that such operations depend on.⁹ Unlike traditional aircraft that function mostly as standalone mechanical systems with human pilots at the helm, eVTOLs are autonomous, highly integrated, data-driven systems.¹⁰ Their operation is closely intertwined with the generation, processing, transmission, and legal governance of data.¹¹ Therefore, any analysis of eVTOL operations must begin from a

⁹ Tingyou Li, Xia Xu & Luyi Shen. (2024) *An Innovation Management Approach for Electric Vertical Take-Off and Landing*. 16 Sustainability 1,3; Saba Al-Rubaye, Antonios Tsoordos & Kamesh Namuduri. (2023) *Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle* 7 Drones 1, 3; Johnny Doo & others. (2021) *NASA Electric Vertical Takeoff and Landing (eVTOL) Aircraft Technology for Public Services – A White Paper*. 20205000636.

¹⁰ Mrinmoy Sarkae & others. (2025) *A Data-Driven Approach for Performance Evaluation of Autonomous eVTOLs*. 61 IEEE Transactions on Aerospace and Electronic Systems 3626, 3627; Lijuan Hu, Xufei Yan & Ye Yuan (2025). *Development and challenges of autonomous electric vertical take-off and landing aircraft*. 11 Heliyon 1, 2.

¹¹ William R. Van Dalsem et al. (2021) *A Data & Reasoning Fabric to Enable Advanced Air Mobility*. 20205011320.

comprehensive examination of the types of data involved, their intended uses, and the regulatory obligations that arise from the technologically distinct features of eVTOLs.¹²

The necessity of continuous real-time communication between different entities involved in the urban air mobility ecosystem is essential to eVTOL operation.¹³ This includes the aircraft itself, its operator, air traffic control systems, regulatory authorities, and in many cases, third-party service providers responsible for identity verification, fleet optimisation, or navigation software.¹⁴ This is in contrast to traditional aviation, where data exchanges are periodic, mostly restricted to flight control and safety procedures, while eVTOL operations require persistent, high-volume data flow.¹⁵ These flows support service delivery, passenger convenience and regulatory compliance, in addition to promoting safe operation. As a result, the legal ramifications extend well beyond traditional aviation law and into areas such as data protection, cybersecurity, and AI governance.¹⁶ To understand these potential complications, it is essential to distinguish the main categories of data involved in eVTOL operations.

The first is **passenger-related data**, which comprises personally identifiable information such as names, contact details, payment credentials, and more recently, biometric data required for access and identity verification. Biometric data, such as fingerprint scans and facial recognition by iris scans, is especially significant in light of modern data protection laws.¹⁷ For example, biometric identifiers are classified as 'sensitive personal data' under the UAE PDPL, which imposes strict requirements for explicit consent, purpose specification, and secure processing.¹⁸ Article 1 of the UAE PDPL states:

¹² Muhammad Yeasir Arafat & Sungbum Pan. (2024) *Urban Air Mobility Communications and Networking: Recent Advances, Techniques, and Challenges* 8 Drones 1, 12.

¹³ Muhammad Yeasir Arafat & Sungbum Pan. (2024) *Urban Air Mobility Communications and Networking: Recent Advances, Techniques, and Challenges* 8 Drones 1, 12.

¹⁴ Annitsa Koumoutsidi, Ioanna Pagoni & Amalia Polydoropoulou. (2022) *A New Mobility Era: Stakeholders' Insights regarding Urban Air Mobility* 14 Sustainability 1, 3.

¹⁵ William R. Van Dalsem et al. (2021) *A Data & Reasoning Fabric to Enable Advanced Air Mobility*. 20205011320; Jordon Golson. (2015) *Why We Don't Need Real-Time Flight Tracking*. Wired. Available from: <https://www.wired.com/2015/01/why-we-dont-need-real-time-flight-tracking/> [Accessed 8 September 2025].

¹⁶ Kenneth Freeman & Steve W. Garcia Jr. (2021) *Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments*. 20205011059; Timothy M. Ravich. (2020) *On-Demand Aviation: Governance Challenges of Urban Air Mobility ("UAM")*. 124 Penn State Law Review. 657, 666.

¹⁷ Shikhar Srivastava, Diwakar Harit & Abhishek Panwar. (2024) *Fingerprints, Iris Scans, and the Law: Regulating Biometric Human-Computer Interfaces*. 9 Journal of Information Systems Engineering & Management. 342, 344; Xukang Wang & others. (2024) *Beyond surveillance: privacy, ethics, and regulations in face recognition technology*. 7 Front. Big Data 1, 2.

¹⁸ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 1.

"Sensitive Personal Data : Any data which directly or indirectly reveals a natural person's family, ethnic origin, political or philosophical opinions, religious beliefs, criminal record, biometric data, or any data relating to such Federal Decree by Law Concerning the Protection of Personal Data 3 person's health and physical, psychological, mental, genetic or sexual condition, including information related to the provision of healthcare services to him/her which reveals his/her health status."

Similar protections for high-risk data categories are reflected in international frameworks like the GDPR of the European Union.¹⁹ Article 9 of GDPR states:

"1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

The second category encompasses **geolocation and environmental data**, which are essential for eVTOLs to navigate safely and efficiently in urban settings.²⁰ For real-time determination of location, altitude, and route, these aircraft rely on complex positioning technologies such as Global Navigation Satellite System (GNSS), inertial measurement units (IMU), and terrain mapping sensors.²¹ At first glance, such data may seem operational rather than personal, but when linked to specific passengers or combined with personally identifiable information to reconstruct movement patterns, it gains legal significance.²² In these instances, location data falls within the protection of PDPL²³ and GDPR,²⁴ both of which acknowledge location as a potentially intrusive form of personal data.

GDPR Article 4 (1) states: *"For the purposes of this Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the*

¹⁹ General Data Protection Regulation 2018, art 9.

²⁰ Nelson Brown et al. (2024) *Visual and Inertial Datasets for an eVTOL Aircraft Approach and Landing Scenario*. 20230016377.

²¹ Paolo Veneruso et al. (2025) *FMCW Radar-Aided Navigation for Unmanned Aircraft Approach and Landing in AAM Scenarios: System Requirements and Processing Pipeline*. 25 *Sensors* 1, 2; Paolo Veneruso et al. (2022) *Sensing Requirements and Vision-Aided Navigation Algorithms for Vertical Landing in Good and Low Visibility UAM Scenarios*. 14 *Remote Sensing*.

²² This is referred to as *Mosaic Effect*, wherein multiple data sources can reveal sensitive information that individual data would not disclose; Rob Matheson. (2018) *The privacy risks of compiling mobility data*. MIT News. Available from: <https://news.mit.edu/2018/privacy-risks-mobility-data-1207> [Accessed 9 September 2025].

²³ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 1.

²⁴ General Data Protection Regulation 2018, art 4 (1).

physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

UAE PDPL Article 1 states: "Personal Data: Any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data, through the use of identification elements such as his/her name, voice, image, identification number, his/her electronic identifier, his/her geographical location, or by one or more physical, physiological, economic, cultural or social characteristics. It includes Sensitive Personal Data and Biometric Data."

Furthermore, the possibility that third parties like state security agencies and private platform providers could obtain this data raises serious ethical questions about surveillance, secondary use, and the unravelling of the purpose limitation principle²⁵ in data protection law.²⁶

Telemetry and operational data make up the third and possibly the largest category of data involved in eVTOL operations. This includes performance metrics such as engine temperature, battery status, altitude, airspeed, and error records—all essential information for airworthiness assessments, predictive maintenance, and incident investigations.²⁷ Such data seems impersonal and technical initially, but when seen in the broader framework of system accountability and liability attribution, its legal status becomes complicated. For example, if an eVTOL malfunction causes passenger injury, telemetry data may be used to determine the sequence of events and determine liability.²⁸ When this data is handled by external third-party vendors or stored in an external cloud environment, concerns arise regarding data ownership,²⁹ admissibility as legal evidence³⁰ and the obligation of data controllers to protect and preserve such information.³¹ These issues are particularly pertinent in light of the UAE PDPL's provisions

²⁵ This principle requires organisations to collect and process personal data only for specific, legitimate reasons.

²⁶ Lubna Luxmi Dhirani et al. (2023) *Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review*. 23 *Sensors* 1, 3; Peter Königs. (2022) *Government Surveillance, Privacy, and Legitimacy*. 35 *Philosophy & Technology*

²⁷ Gaurav Gowda Babu Yashoda et al. (2025) Predictive Maintenance of Aircraft Engine Failure. 5 *International Journal of Advanced Multidisciplinary Research and Studies*; Mihaela Mitici et al. (2024) *Predictive Maintenance Planning for Batteries of Electric Take-Off and Landing (eVTOL) Aircraft Using State-of-Health Prognostics*. European Safety and Reliability Conference.

²⁸ Gábor Vida & Árpád Török. (2023) Expected effects of accident data recording technology evolution on the identification of accident causes and liability. 15 *European Transport Research Review*. 1, 12.

²⁹ Dennis B Park et al. (2021) Data ownership in cloud: legal issues. 1 *International Journal of Forensic Engineering & Management*. 1, 2.

³⁰ Munirah Maher Alshabibi, Alanood Khaled Bu dookhi & M. M. Hafizur Rahman (2024) *Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review*. 13 *Computers* 1, 3.

³¹ Christos Karagiannis & Kostas Vergidis. (2021) *Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal*. 12 *Information* 1, 6.

on joint controllership and processor obligations, which impose strict duties on entities that determine the purpose of processing, whether individually or jointly.³²

Across all three data categories, the challenge of real-time transmission and interconnectivity introduces an additional layer of legal complexity. eVTOLs cannot operate in isolation; they need constant contact with ground-based infrastructure to navigate, avoid collisions, and integrate into urban air traffic systems. Despite being essential for operations, this connectivity creates legal vulnerabilities related to cybersecurity and system resilience. For example, if geolocation data is compromised through signal spoofing, the repercussions could be anything from physical harm to privacy concerns.³³ Article 20 of the UAE PDPL³⁴ mandates “*appropriate technical and regulatory measures to ensure the highest standard of information security*”; however, it is unclear what exactly qualifies as appropriate, particularly in the context of autonomous aviation.

This challenge is exacerbated by the divided nature of liability within the eVTOL ecosystem. One organisation may collect data (ride-hailing app), another may process it (facial recognition vendor), a third may transmit it (telecommunications provider), and a fourth may store it (cloud system platform). In such situations, robust contractual agreements, real-time auditing tools, and sector-specific codes of practice are essential to guarantee adherence to the UAE PDPL’s accountability and transparency principles.³⁵ Without these mechanisms, judicial courts may find it challenging to determine liability for data misuse, breach or system failure.

The increasing reliance on AI-driven decision-making in eVTOL operations creates legal problems because autonomous systems execute real-time actions without human intervention in critical safety scenarios. Both the UAE PDPL³⁶ and the GDPR³⁷ recognise the necessity of restricting such fully automated decisions when they have substantial or legal effects on individuals.

Article 18 of the UAE PDPL states:

³² Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, arts. 14-16.

³³ Shah Zahid Khan, Mujahid Mohsin & Waseem Iqbal. (2021) On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *Computer Science*, 1, 11.

³⁴ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 20.

³⁵ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data.

³⁶ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 18.

³⁷ General Data Protection Regulation 2018, art 22.

"1. The Data Subject shall have the right to object to any decisions resulting from automated processing, including profiling, particularly those decisions which have legal impact on or adversely affect the Data Subject.

2. Notwithstanding Paragraph 1 of this Article, the Data Subject may not object to the decisions resulting from automated processing in the following cases:

- a. If the automated processing is agreed upon under the contract made between the Data Subject and the Controller.*
- b. If the automated processing is required under other legislations which are applicable in the State.*
- c. If the Data Subject gives prior consent to the automated processing as set out in Article (6) of this Decree by Law.*

3. The Controller shall adopt appropriate measures to protect the privacy and confidentiality of the Data Subject's Personal Data in the cases referred to in Paragraph 2 of this article and shall not cause any prejudice to the Data Subject's rights

4. The Controller shall include the human element in reviewing automated processing decisions at the request of the Data Subject."

Article 22 of GDPR states:

"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

- (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
- (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
- (c) is based on the data subject's explicit consent.*

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

However, the UAE PDPL does not provide comprehensive guidelines on how these rights are to be operationalised, in contrast to the GDPR, which mandates certain procedural safeguards, including the right to human oversight, explanation, and contestation.³⁸ In autonomous eVTOLs, this raises particular concerns as algorithmic decisions regarding emergency rerouting or system overrides may have an impact on passengers without providing them with effective avenues for redress.

These complexities illustrate that eVTOLs cannot solely be treated as an aviation innovation but as a contemporary data governance challenge. Yet, scholarly research to address these intersections is still in its earliest phases. The following section reviews existing scholarship on eVTOLs, data protection and aviation cybersecurity to identify what has been explored and where gaps remain.

3. LITERATURE REVIEW

Sharing data online has become part of our daily lives. At times, we do it mindlessly without putting much thought into whether our data is protected or not. This makes data protection of utmost importance in today's day and age. With the development of urban air mobility (UAM) as a new mode of transport in the shape of eVTOLs, there has been an enhancement in air mobility.³⁹ eVTOLs promote sustainability because they operate on batteries rather than fuel, improve traffic management, and feature eco-friendly aircraft designs with lower carbon dioxide levels.⁴⁰

However, eVTOLs are vulnerable to a number of cyber threats due to their digital interference and communication networks.⁴¹ To obtain unauthorized access, malicious actors can take advantage of flaws in communication protocols, control systems, and vehicle software. Sensitive information may be included in data transferred between infrastructure and aircraft, making data privacy and encryption crucial for transportation security.⁴² For the

³⁸ *General Data Protection Regulation 2018*, art 22 (3).

³⁹ Pablo Mendes de Leon & Benjamyn Scott. (2023) Scanning the Air Transport Market in Europe and Beyond: The Position of Airlines and the Evolution of Technical Innovations in Alan D. Meneghetti & Philip Perrotta. (eds.) *International Comparative Legal Guides*. 15, 17.

⁴⁰ Pablo Mendes de Leon & Benjamyn Scott, 'Scanning the Air Transport Market in Europe and Beyond: The Position of Airlines and the Evolution of Technical Innovations' in Alan D. Meneghetti & Philip Perrotta (eds), *International Comparative Legal Guides* (Global Legal Group 2023) 15, 17.

⁴¹ Lubna Luxmi Dhirani, Eddie Armstrong & Thomas Newe. (2021) *Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap* 11 Sensors 1, 3.

⁴² Gulshan Kumar & Ali Altalbe. (2024) *Artificial intelligence (AI) advancements for transportation security: in depth insights into electric and aerial vehicle systems*. *Environment, Development and Sustainability* 1, 8.

successful long-term integration of eVTOLs, it is essential for them to be a secure form of advanced air mobility (AAM) transport.

Scholars highlight the importance of addressing concerns relating to privacy, i.e., collection, transmission and storage of data collected by eVTOLs.⁴³ They stress the necessity of regulations regarding cybersecurity, liability and insurance to safeguard passengers while maintaining operational safety and security.⁴⁴ Data from AI-enabled systems used for real-time navigation must be protected to prevent misuse and inconvenience to passengers.⁴⁵ A suggestion has also been put forward to introduce privacy-preserving machine learning tools such as differential privacy, secured data sharing protocol and homomorphic encryption to safeguard sensitive data collected by eVTOLs during the course of their operation.⁴⁶

However, the existing literature remains largely fragmented. Most studies focus on technical safeguards in isolation and do not assess how these measures fit within a coherent regulatory framework or interact with broader data protection principles under instruments like the UAE PDPL and the GDPR. Many also assume that advanced privacy-enhancing tools can be implemented without addressing practical, operational or jurisdictional challenges.

In a research conducted in Türkiye, the people interviewed had concerns about eVTOLs susceptibility to hackers, they emphasized that dangers such as eVTOL abuse and hacking, may result in privacy violations and the exploitation of private information. The article reveals the necessity of strong cybersecurity safeguards to guarantee safe data handling and stop illegal access while using eVTOLs.⁴⁷ While these concerns reflect broader global debates, the literature rarely considers how such cybersecurity risks should be addressed within existing aviation and data protection frameworks or who should be held accountable. This gap shows that although risks are recognised, their regulatory implications remain underexplored.

Some scholars have also suggested that the regulatory framework governing eVTOLs in different countries, i.e., the USA and EU,

⁴³ Ridha Nugraha & Benjamyn Scott. (2024) *Flying taxis, air mobility and challenges for Indonesia*. The Jakarta Post. Available from: <https://scholarlypublications.universiteit.leiden.nl/access/item/%3A3728443/view> [Accessed 17 November 2025.]

⁴⁴ Ridha Nugraha & Benjamyn Scott. (2024) *Flying taxis, air mobility and challenges for Indonesia*. *op. cit.*

⁴⁵ Sakshi Mishra & Praveen Palanisamy. (2023) *Autonomous Advanced Aerial Mobility—An End-to-End Autonomy Framework for UAVs and Beyond*. 11 IEEE Access 318, 320.

⁴⁶ Sakshi Mishra & Praveen Palanisamy. (2023) *op. cit.*; Hamed Alqahtani & Gulshan Kumar. (2024) *Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems*. 29 Engineering Applications of Artificial Intelligence.

⁴⁷ Ertan Çınar & Arif Tuncal. (2023) *The Future of UAVs in Urban Air Mobility: Public Perception and Concerns*. *Turkish Journal of Unmanned Aerial Vehicles*. 50, 54.

should be collaborated in order to ensure safety with a keen focus on airspace management, liability and certification.⁴⁸ But these calls for cross-jurisdictional alignment often overlook the substantial differences between national legal systems, particularly in data protection, liability allocation and certification standards. Without resolving these procedural differences, meaningful regulatory harmonisation remains difficult. This reveals the need for each jurisdiction, including the UAE, to assess how international laws can be adapted within its own legal framework while ensuring interoperability and safety.

In the EU, data protection is governed by GDPR. It has been suggested that adherence to GDPR for managing data privacy will lead to a more secure urban air mobility ecosystem.⁴⁹ The principles of Article 5⁵⁰ on lawfulness, fairness, transparency and integrity of processing data are particularly relevant to eVTOL data, while Article 22⁵¹ on automated decision making and profiling have direct implications for AI-based navigation systems. Moreover, the strict requirements for cross-border data transfers provided under Articles 44 to 50 highlight the challenge of international operability of UAM data.⁵²

Even though eVTOLs offer a chance to boost transportation capacity in crowded cities, public acceptability is crucial to their successful integration into current transportation networks. However, the public has a psychological fear of the unknown when it comes to flying taxis.⁵³ Public hesitation is acknowledged but it is rarely connected to how safety rules, data protection standards and transparency measures should be designed to build trust, therefore, while public concerns are documented, their translation into regulatory responses remains underexplored.

Furthermore, it is also important to enhance transparency and accountability to build trust amongst the general public.⁵⁴ In this regard,

⁴⁸ Sakshi Mishra & Praveen Palanisamy. (2023) Autonomous Advanced Aerial Mobility—An End-to-End Autonomy Framework for UAVs and Beyond. *op. cit.*

⁴⁹ Konstantinos Andritsos, Benjamyn Scott & Andrea Trimarchi. (2022) What is in a Name: Defining Key Terms in Urban Air Mobility. *Journal of Intelligent & Robotic Systems*.

⁵⁰ *General Data Protection Regulation 2018*, art. 5.

⁵¹ *General Data Protection Regulation 2018*, art. 22.

⁵² *General Data Protection Regulation 2018*, art. 44-50.

⁵³ Ricole Johnson, Erika Miller & Steven Conrad. (2022) Technology Adoption and Acceptance of Urban Air Mobility Systems: Identifying Public Perceptions and Integration Factors. *The International Journal of Aerospace Psychology*, 240.

⁵⁴ Andrea Trimarchi. (2023) *Technological Certainties and Regulatory Doubts: An Overlook at Unmanned Aviation and Urban Air Mobility in Europe*. International Conference on Unmanned Aircraft Systems, Poland, June 2023.

transparency obligations under Articles 12 to 14 of GDPR and Article 5 of the UAE PDPL⁵⁵ can be seen as tools to foster such trust.

Even though the US does not have a federal law comparable to the GDPR, the FAA has incorporated cybersecurity considerations into its UAS and advanced air mobility initiatives through certification requirements.⁵⁶ However, binding regulations are still under development. Additionally, frameworks such as the NIST Cybersecurity Framework (National Institute of Standards and Technology)⁵⁷ are frequently referenced in aviation security scholarship, yet the absence of a comprehensive privacy legislation leaves a significant regulatory gap for passenger data in eVTOLs.⁵⁸

In the UAE, the Federal Decree No. 45 of 2021 on the Protection of Personal Data (PDPL) is the foundational framework for data governance. It encompasses the fundamental principles of lawfulness, consent, purpose limitation, and data subject rights, all of which directly influence how passenger identifiers, geolocation, and communication data are gathered and processed during eVTOL operations. The General Civil Aviation Authority (GCAA) has separately issued circulars on aviation cybersecurity that intersect with the protection of eVTOL data systems.⁵⁹ Although the UAE PDPL provides a comprehensive legal groundwork, aviation presents unique challenges that call for industry-specific regulations. As eVTOL operations entail a constant flow of cross-border data, which is critical for safety that links multiple stakeholders, making data breaches not only a privacy issue but also a safety and operational risk. Therefore, by integrating cybersecurity and privacy into certification and liability frameworks, aviation-specific data protection measures not only complement but also enhance the UAE PDPL.

Although data governance issues have started to be explored in existing eVTOL research, the discussion remains uncoordinated. Much of the scholarly literature discusses generic data protection frameworks, including the GDPR, but it seldom pays close attention to how these concepts relate to

⁵⁵ *Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data*, art 5.

⁵⁶ Federal Aviation Administration. (2020) *FAA Cybersecurity Strategy*. [online] Available from: <https://www.faa.gov/about/plansreports/faa-cybersecurity-strategy> [Accessed 27 August 2025].

⁵⁷ National Institute of Standards and Technology. (2024) *The NIST Cybersecurity Framework*. [online] Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [Accessed 26 August 2025].

⁵⁸ Filiz Mizrak & Gonca Reyhan Akkartal. (2024) *Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology*. 10 Heliyon 1, 5.

⁵⁹ General Civil Aviation Authority. (2024) *GCAA National Aviation Cybersecurity*. [online] Available from: <https://www.gcaa.gov.ae/en/epublication/PublishingImages/Pages/gcaa-cyber-security/GCAA\%20National\%20Civil\%20Aviation\%20Cybersecurity\%20Guidelines\%20Version\%201\%20Sept\%202024.pdf> [Assessed 27 August 2025].

the aviation industry.⁶⁰ Data protection is often treated as incidental rather than as a standalone regulatory issue in aviation law, which has historically focused on certification, safety, and liability.⁶¹ Additionally, there is little comparative analysis of how different jurisdictions like the US, EU, and the UAE handle the nexus of data protection with aviation cybersecurity.⁶² Notably, despite their ambitious smart mobility initiatives, the UAE and the wider MENA (Middle East & North Africa) region remain largely absent from the academic discourse, and the literature gives minimal consideration to how personal passenger data and safety-critical operational data in eVTOL systems should be differentiated and governed within domestic legal frameworks.⁶³ This gap is notable because, to guarantee trust and operational resilience in deploying eVTOLs, domestic regulatory readiness and the synchronization of data protection and cybersecurity measures exclusive to the aviation sector will be crucial. Thus, this article provides a doctrinal analysis of eVTOL data governance in the UAE, situating the discussion comparatively against the more developed cybersecurity and data protection regimes of the EU and the US.

4. UAE LEGAL LANDSCAPE FOR DATA PROTECTION AND AVIATION CYBERSECURITY

The successful integration of eVTOLs within the UAE's urban mobility framework depends not only on technical viability but on the clarity, adaptability and enforceability of the country's data protection and cybersecurity regulations.⁶⁴ Since eVTOL operations are particularly data-intensive and autonomous, traditional aviation laws now have to interact with much more comprehensive digital governance instruments.⁶⁵

⁶⁰ W. Gregory Voss. (2020) Cross-Border Data Flows, the GDPR, and Data Governance. *Washington International Law Journal*, 485, 489; W. Gregory Voss. (2021) Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems. *Colorado Technology Law Journal*, 377.

⁶¹ Geetika Kapil. (2025) Cybersecurity Challenges in Aviation. *European Journal of Advances in Engineering and Technology*; Eric Ekström. (2025) *Cybersecurity Challenges to Airlines: A Literature Review of Risk & Compliance*. Bachelors thesis, Lund University.

⁶² Eugénie Coche, Ans Kolk & Václav Ocelík. (2024) Unravelling cross country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 112, 115-117.

⁶³ Alaa Abouahmed, Moustafa Elmetwaly Kandeel & Aliaa Zakaria. (2024) Personal Data Protection In The United Arab Emirates and the European Union Regulations. *Journal of Governance & Regulation*, 195, 196.

⁶⁴ Paola Di Mascio, Giulia Del Serrone & Laura Moretti. (2025) *Vertiports: The Infrastructure Backbone of Advanced Air Mobility — A Review*. 6 Eng 1, 2; Yannan Lu et al. (2025) Urban Air Mobility Vertiports: A Bibliometric Analysis of Applications, Challenges, and Emerging Directions. *Applied Sciences* 1, 18.

⁶⁵ Robert Notari. (2025) Autonomy Now?: Is It Time To Start Integrating (Autonomous) Urban Air Mobility Vehicles Into The National Airspace System? *Texas A&M Law Review*, 52, 63;

The Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and other regional cybersecurity standards serve as the foundation for digital regulation in the UAE.⁶⁶ Nevertheless, these instruments remain insufficiently developed to handle the unique requirements of advanced autonomous air mobility systems.

Article 2 of the UAE PDPL⁶⁷ reads:

"1. Provisions of this Decree by Law shall apply to the processing of all or part of the Personal Data by means of electronic systems which operate automatically, or by other means, by the following:

- a. Each Data Subject residing in the State or having a place of business in it.*
- b. Each Controller or Processor residing in the State and carrying out the activities of processing Personal Data of Data Subjects inside and outside the State.*
- c. Each Controller or Processor residing outside the State and carrying out the activities of processing Personal Data of Data Subjects inside the State."*

This article's extraterritorial reach guarantees that the PDPL applies to numerous international eVTOL stakeholders, including foreign service providers that handle data about residents of the UAE. However, unlike traditional air traffic processes, where data flows are periodic and jurisdictionally restricted, eVTOL services rely on real-time, distributed processing that will frequently use multinational cloud infrastructure.⁶⁸ This raises urgent questions about how to meet the UAE PDPL's requirement without jeopardizing operational continuity, including demonstrable safeguards and government approval for data transfer in the event of inadequacy.

Furthermore, while earlier sections of the article have addressed how biometric data and geolocation are treated under the UAE PDPL's substantive provisions, less attention has been placed on how governance obligations are operationalised across multiple actor ecosystems. As noted earlier,

Ruwantissa Abeyratne. (2024) Advanced Air Mobility: Transcending the Frontiers of Aviation Law. *Frontiers in Law*, 90, 91.

⁶⁶ Maitha Musabah Salem Bin Dhawi Al Khateri & Diaya Ud Deen Deab Mahmoud Al Zitawi. (2025) Cybersecurity and Protection of Digital Data Privacy in the UAE in the Age of Digital Transformation and Artificial Intelligence. *International Journal of Academic Research in Business & Social Sciences*, 491, 498.

⁶⁷ *Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data*, art 2.

⁶⁸ Karnika Biswas et al. (2023). Urban Air Mobility: An IoT Perspective. *IEEE Internet of Things Magazine*, 122, 123; Saba Al-Rubaye, Antonios Tsourdos & Kamesh Namuduri. (2023) *Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle*, 7 Drones 1, 4.

several players are involved in eVTOL operations, including cloud vendors, AI service integrators, digital infrastructure providers and the operator itself.⁶⁹ The UAE PDPL assigns independent obligations to both controllers and processors under Articles 9, 10 and 11. These articles govern breach notification, processing duties and contractual obligations. However, they do not impose joint liability across these roles. Consequently, liability in a multi-actor eVTOL ecosystem is likely to depend on the facts of a particular incident, the allocation of responsibilities in contracts and judicial interpretation.⁷⁰

This regulatory vacuum becomes more profound in the field of aviation cybersecurity, where national strategies and advisory documents remain essentially non-binding.⁷¹ The GCAA's National Civil Aviation Cybersecurity Guidelines are voluntary and not tailored to the architectural and operational risks posed by eVTOL systems.⁷² Enforceable standards for third-party application programming interface (API) testing, flight-critical software security, and encryption requirements for telemetry data transferred between airborne and ground-based systems are notably non-existent.⁷³ On the other hand, jurisdictions like the EU have started incorporating such standards into the type certification process of eVTOLs, making cybersecurity a fundamental component of airworthiness evaluations.⁷⁴ Another emerging challenge is the UAE PDPL's treatment of automated decision-making. Similar to Article 22 of the GDPR, Article 18 of UAE PDPL recognises a person's right not to be subject to fully automated decisions

⁶⁹ Saba Al-Rubaye, Antonios Tsourdos & Kamesh Namuduri. (2023) *Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle*. Drones 1, 14; Adam Mitchell and Robin Riedel. (2022) *Building digital platforms to enable advanced air mobility*. [online] McKinsey & Company. Available from: <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/building-digital-platforms-to-enable-advanced-air-mobility> [Accessed 23 October 2025].

⁷⁰ Benjamyn I. Scott & Öykü Kurtpınar. (2025) Hoffnungen und Hürden: Regulatorische Herausforderungen für Advanced Air Mobility. *Advanced Air Mobility* (5.1) and *Advanced Air Mobility* (5.2); Timothy M. Ravich. (2020). On-Demand Aviation: Governance Challenges of Urban Air Mobility ("UAM"). *Penn State Law Review* 657, 672.

⁷¹ Calvin Nobles, Darrell Burrell & Tyrone Waller, (2022) The Need for A Global Aviation Cybersecurity Defense Policy. *Land Forces Academy Review* ; Elochukwu Ukwandu and others, (2022) *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends* 13 Information 1, 2.

⁷² General Civil Aviation Authority. (2025) *GCAA National Aviation Cybersecurity*. [online] Available from: <https://www.gcaa.gov.ae/en/epublication/Pages/gcaa-cyber-security.aspx> [Accessed 23 October 2025].

⁷³ General Civil Aviation Authority, (2023) *The UAE Civil Aviation Cybersecurity Policy* Available from: <https://www.gcaa.gov.ae/en/epublication/Shared/%20Documents/UA E%20CIVIL%20AVIATION%20CYBERSECURITY%20POLICY%20Issue%201.pdf> [Accessed 23 October 2025].

⁷⁴ EUR-Lex, (2022) *Commission Implementing Regulation (EU) 2023/203* Available from: https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj [Accessed 23 October 2025].

that have substantial or legal ramifications. The UAE framework recognises human review but provides insufficient procedural detail concerning when, how and according to what standards that review must occur in risky aviation contexts.⁷⁵ In practice, passengers affected by real-time automated decisions, such as emergency diversions or denial of boarding due to AI risk assessments, currently lack a structured mechanism to request human review or contest outcomes.⁷⁶ When the decision in question directly affects safety or dignity, as is frequently the case in AI-governed air mobility, this procedural gap becomes legally and ethically challenging.⁷⁷

Although acknowledged as a national matter, cyber-resilience is not yet standardised at the aviation-system level.⁷⁸ This puts eVTOL operators in a legal limbo where adherence to Article 21 of the UAE PDPL, which requires appropriate technical and organisational measures, is necessary but unclear. While large-scale operators voluntarily adopt industry best practices or use standards like ISO 27001⁷⁹ or the NIST Cybersecurity Framework,⁸⁰ there is no binding aviation sector benchmark in the UAE against which such measures can be audited. This could lead to the emergence of compliance asymmetry, whereby only highly resourceful providers can afford to meet global cybersecurity standards.⁸¹ This would exclude start-up innovators or discourage foreign operators who are uncertain of how the UAE compliance will be interpreted in a high-risk environment.

Lastly, there is a structural issue of regulatory fragmentation. While the UAE PDPL is administered by the UAE Data Office,⁸² cybersecurity oversight is divided among the UAE Cybersecurity Office, Telecommunications

⁷⁵ *Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data*, art 18.

⁷⁶ Pericle Salvini and others, (2023) Human involvement in autonomous decision-making systems. Lessons learned from three case studies in aviation, social care and road vehicles *Frontiers in Political Science* 1, 13.

⁷⁷ Jakob Mokander and others, (2021) Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations. *Science and Engineering Ethics* 1, 16.

⁷⁸ General Civil Aviation Authority, (2023) *The UAE Civil Aviation Cybersecurity Policy* Available from: <https://www.gcaa.gov.ae/en/epublication/Shared%20Documents/UA E%20CIVIL%20AVIATION%20CYBERSECURITY%20POLICY%20Issue%201.pdf> [Accessed 23 October 2025].

⁷⁹ ISO. (2022) [online] ISO.org. Available from: <https://www.iso.org/standard/27001> [Accessed 7 October 2025].

⁸⁰ National Institute of Standards and Technology, (2024) *The NIST Cybersecurity Framework* [online] nvlpubs.nist.gov. Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [Accessed 26 August 2025].

⁸¹ Kingsford Brakye & Abdul Basit Karim Adam, (2025) Cybersecurity Risk Disclosure and Regulatory Compliance: Evaluating Market Sensitivity and Disclosure Effectiveness in U.S. Public Companies *EPRA International Journal of Economics, Business and Management Studies*.

⁸² The UAE Government. (2024) *Data protection laws*. [online] The UAE Government Portal. Available from: <https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws> [Accessed 7 October 2025].

and Digital Government Regulatory Authority (TDRA), Dubai Electronic Security Centre (DESC) and the GCAA.⁸³ Because eVTOL systems function at the nexus of transport, data, AI governance and infrastructure, the absence of harmonised supervisory mechanisms may lead to inconsistent interpretations, redundant obligations or enforcement gaps.⁸⁴

Therefore, while the PDPL and the sectoral cybersecurity frameworks provide a valuable foundation for eVTOL system regulation, they do not yet reflect the technological foresight, operational peculiarity and sectoral depth needed for this emerging domain. Key provisions, particularly those related to automated decision-making, multi-actor liability and cross-border data flows, remain underdeveloped and untested. In the absence of binding aviation-specific regulations or a uniform supervisory strategy, there is an imminent risk of regulatory misalignment with both international standards and operational realities.

5. KEY LEGAL AND POLICY CHALLENGES IN EVTOL DATA GOVERNANCE

Many of the challenges identified below are not unique to eVTOL operations, they occur across autonomous and semi-autonomous aviation, including drone traffic management.⁸⁵ What sets apart eVTOLs is the combination of high passenger volume, proximity to dense urban population and the routine collection of passenger-linked biometric and geolocation data as a condition of boarding. These features are largely absent from cargo drones or other autonomous aircraft that do not carry passengers.

Along with new technology, the eVTOL ecosystem brings with it an entirely new mode of data production and circulation- data that is both operational and sensitive, personal and infrastructural, local and transnational, which in turn leads to new legal consequences.⁸⁶ This creates

⁸³ The UAE Government. (2024) *Cyber safety and digital security*. [online] The UAE Government Portal. Available from: <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security> [Accessed 7 October 2025].

⁸⁴ Esmat Zaidan & Imad Antoine Ibrahim. (2024) AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanities and Social Sciences Communication*; Lachlan Robb et al. (2023) Regulatory overlap: A systematic quantitative literature review. *Regulation and Governance*; Daria Gritsenko & Matthew Wood. (2020) Algorithmic governance: A modes of governance approach. *Regulation and Governance*.

⁸⁵ Panagiotis Aposporis, (2024) *A review of global and regional frameworks for the integration of an unmanned aircraft system in air traffic management* 24 *Transportation Research Interdisciplinary Perspectives* 1, 11; Nichakorn Pongsakornsathien et al. (2025) *Advances in low-altitude airspace management for uncrewed aircraft and advanced air mobility*. 154 *Progress in Aerospace Sciences* 1, 20.

⁸⁶ Dimitrios Ziakkas & others, (2025) *Designing human-centric intelligent systems in aviation: applications of artificial cognitive systems, AI-enhanced investigations, and immersive eVTOL*

unprecedented challenges for regulators in the USA, the EU and the UAE when it comes to categorizing, securing and governing data produced by autonomous or semi-autonomous aerial systems.

This section presents six under-addressed challenges in the current UAE regulatory landscape, each compounded by the unique legal interplay between airworthiness, AI governance and personal data protection. By using comparative insights from the more advanced yet developing legal systems of the USA and the EU, these challenges are examined not as mere compliance concerns but as structural deficiencies in the normative framework of eVTOL governance.

5.1. AMBIGUITY IN DATA CLASSIFICATION

Data collected by the eVTOL systems will be used both for personal identification and operational safety. Telemetry logs, real-time geolocation and biometric access systems blur the line between aviation data and personal data, making it challenging to determine which legal framework governs their use.⁸⁷ Unlike the EU, where tiered compliance frameworks are emerging under GDPR and EASA instruments, the UAE lacks a consistent classification standard or regulatory interpretation that clarifies the legal status of hybrid datasets.⁸⁸ The uncertainty raises the possibility of conflicting obligations or regulatory overreach, particularly when flight data is retrospectively analysed for liability or national security purposes.⁸⁹ For consistent and predictable compliance, the distinction between privacy-sensitive and safety-critical data streams must be more clearly defined.

simulation training Human-Intelligent Systems Integration; Francesca Castaldo and others, *Urban Air Mobility: Organisation and Governance of a Frontier Ecosystem* (IFKAD 2024: Translating Knowledge into Innovation Dynamics, Madrid Spain, 12-14 June 2024) Available from: https://www.researchgate.net/publication/382021028_Urban_Air_Mobility_Organisation_and_Governance_of_a_Frontier_Ecosystem [Accessed 28 October 2025.]

⁸⁷ A. Chebotareva and others, (2023) *Personal data protection in the civil aviation industry: Technological challenges and legal efforts* 2526 *Modern Approaches in Engineering and Natural Sciences*.

⁸⁸ EASA. (2024) *EASA Concept Paper: guidance for Level 1 & 2 machine learning applications*. 2nd ed. Available from: <https://horizoneuropencpportal.eu/sites/default/files/2024-06/easa-concept-paper-guidance-for-level-1-and-2-machine-learning-applications-2024.pdf> [Accessed 29 October 2025]; Ana Beduschi, (2024) *Synthetic data protection: Towards a paradigm change in data regulation?* 11 *Big Data & Society*; Nadezhda Purtova, (2018) *The law of everything. Broad concept of personal data and future of EU data protection law* 10 *Law, Innovation & Technology*.

⁸⁹ Igor Kabashkin & Vitaly Susanin, (2024) *Unified Ecosystem for Data Sharing and AI-Driven Predictive Maintenance in Aviation* 13 *Computers*.

5.2. FRAGILITY OF CONSENT MECHANISMS

The operational architecture of eVTOL requires rapid, multi-actor data processing, often across jurisdictional borders.⁹⁰ Under such circumstances, the model of legal consent under the UAE PDPL, which relies on prior, informed and explicit user approval, is difficult to operationalise meaningfully.⁹¹ While the GDPR has begun to acknowledge contextual and layered consent models, the UAE PDPL does not yet accommodate dynamic data processing shifts during the course of a trip.⁹² As data moves between ride-hailing apps, cloud vendors and onboard AI modules, it becomes unclear whether original consent terms remain legally effective.⁹³ Consequently, even when data processing is done in good faith, operators are at risk of non-compliance, undermining the principle of user autonomy.

5.3. GAPS IN PRIVATE-PUBLIC DATA SHARING

The UAE's smart mobility initiatives depend on integrating eVTOL platforms with state infrastructure, such as emergency response systems, municipal mobility grids and airspace regulators.⁹⁴ However, there is no specific legal framework that regulates the exchange of data or the division of obligations between public authorities and private manufacturers and operators.⁹⁵ This contrasts with the US FAA's municipal coordination models and the EU's emerging interoperability frameworks under the GDPR, Data Act and EASA instruments.⁹⁶ The lack of legal instruments defining shared responsibility and proportionality in public-private data flows risks inconsistent data

⁹⁰ Nabih Naeem, (2025) *A collaborative system of systems simulation of urban air mobility* 16 CEAS Aeronautical Journal.

⁹¹ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 6.

⁹² General Data Protection Regulation 2018, arts. 5-11.

⁹³ Soheil Human, (2022) *Advanced Data Protection Control (ADPC): An Interdisciplinary Overview* arXiv Available from: <https://arxiv.org/abs/2209.09724> [Accessed 30 October 2025]; Sandra Wachter & Brent Mittelstadt, (2019) *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*. *Columbia Business Law Review*; Shoshana Zuboff. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st Ed. Public Affairs, p. 159.

⁹⁴ Mohammad Owais Farooqui, (2025) *Rooftop Runways: Evaluating the UAE's Regulatory Framework for Vertiports in Urban Air Mobility*. *Via Inveniendi Et Iudicandi* 149, 153.

⁹⁵ Mohammad Abu-Matar & John Davies, *Data Driven Reference Architecture for Smart City Ecosystems* (17 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, San Francisco, USA) Available from: <https://ieeexplore.ieee.org/abstract/document/8397556> [Accessed 3 November 2025.]

⁹⁶ Pieter T.J. Wolters, (2024) *The Influence of the Data Act on the Shifting Balance between Data Protection and the Free Movement of Data*. *European Journal of Law & Technology*; European Commission, *Data Act Explained* (European Commission, 12 September 2025) <<https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained> [Accessed 3 November 2025.]

privacy enforcement and systemic accountability.⁹⁷ In order to guarantee transparency, trust and compliance without drastically limiting innovation, regulatory action will be essential as these partnerships establish themselves.

5.4. LACK OF ALGORITHMIC ACCOUNTABILITY

Autonomous eVTOL systems rely on third-party AI tools to determine routing, altitudes and emergency responses. Despite acknowledging automated decision-making,⁹⁸ the UAE PDPL lacks mandatory transparency or human oversight. The GDPR and EASA guidance provide more tangible safeguards against unaccountable algorithmic decisions, particularly in high-risk contexts.⁹⁹ In the absence of these safeguards, when algorithmic errors occur, liability becomes obscure, making legal redress nearly impossible.¹⁰⁰ The UAE should consider adopting algorithmic accountability standards like the GDPR to ensure traceability, fairness and legal oversight in AI-enabled flight operations.

5.5. LACK OF PROCEDURAL PATHWAYS FOR EVTOL DISPUTES

Although eVTOL services in the UAE will operate within national borders, there is currently no clear legal framework in place for resolving disputes related to data generated and collected through these systems.¹⁰¹ Neither the UAE PDPL nor the existing GCAA instruments have a specific procedure for handling incidents involving privacy breaches, cybersecurity failures or algorithmic decision-making errors.¹⁰² Complaints would likely be distributed across multiple regulatory bodies, creating uncertainty for both operators and affected individuals.¹⁰³ Furthermore, there is no administrative procedure or specialised forum that can handle the technical complexities of aviation data disputes, including issues involving cloud

⁹⁷ Esin Küçük & Elif Mendos Kuşkonmaz, (2025) Solidarity at the intersection of data sharing and data protection: A normative analysis. *Maastricht Journal of European and Comparative Law*.

⁹⁸ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 18.

⁹⁹ General Data Protection Regulation 2018, art. 22.

¹⁰⁰ Will Fleisher and others, (2025) Responsibility and Accountability in an Algorithmic Society *Philosophy & Technology*; Zoya Yousef, (2024) How Can the Law Address the Effects of Algorithmic Bias in the Healthcare Context? *LSE Law Review*.

¹⁰¹ Alaa Abouahmed, Moustafa Elmetwaly Kandeel & Aliaa Zakaria, (2024) Personal Data Protection In The United Arab Emirates and the European Union Regulations. *Journal of Governance & Regulation*; Ahmed Al-Fahim & Fatima Al-Zaabi, (2024) Artificial Intelligence in Law and Ethics in the United Arab Emirates: Balancing Innovation, Regulation, and Cultural Values. *Future Publishing House*.

¹⁰² General Civil Aviation Authority, (2023) *The UAE Civil Aviation Cybersecurity Policy* Available from: <https://www.gcaa.gov.ae/en/epublication/Shared%20Documents/UAEE%20CIVIL%20AVIATION%20CYBERSECURITY%20POLICY%20Issue%201.pdf> [Accessed 23 October 2025.]

¹⁰³ Jinghui He & Zhenyang Zhang, (2025) *Algorithm Power and Legal Boundaries: Rights Conflicts and Governance Responses in the Era of Artificial Intelligence* 14 *Laws* 1, 19.

service providers or AI vendors.¹⁰⁴ A defined procedural framework would improve accountability and facilitate predictable enforcement outcomes, potentially through the use of a specialised aviation data dispute mechanism.

5.6. EVOLVING LEGAL FRAMEWORKS FOR EMERGING TECHNOLOGIES

As the UAE advances its vision for autonomous mobility, the regulatory framework for eVTOL-related data would benefit from more flexible and participatory mechanisms. Compared to emerging models in the EU and the USA that increasingly incorporate regulatory sandboxes and multistakeholder consultations, the UAE's approach remains largely centralised.¹⁰⁵ Although this has supported rapid policy development, it may have drawbacks in domains where cross-sectoral complexity and swift technology advancement are prevalent.¹⁰⁶ Organised forums with industry and technology experts could boost innovation, improve compliance outcomes and increase regulatory foresight. Developing flexible, evolving legal instruments would ensure that the governance of eVTOL systems remains responsive, balanced and aligned with both technological change and public expectations.

6. EVOLVING INTERNATIONAL APPROACHES TO EVTOL DATA GOVERNANCE

Building on the gaps identified in the UAE's existing legal framework, this section examines how the EU and the USA have approached comparable challenges in regulating data within advanced air mobility (AAM) systems.¹⁰⁷ Although no jurisdiction has yet established a dedicated legal framework for eVTOL data governance, both regions have developed evolving regulatory and institutional instruments that indirectly shape the governance of data, cybersecurity and artificial intelligence within

¹⁰⁴ Ugo Pagallo & Eleonora Bassi, (2020) *The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human Rights, and the Free Movement of Data in the EU (2020) 30 Minds and Machines*.

¹⁰⁵ Thiago Moraes, (2024) *Ethical AI Regulatory Sandboxes: Insights from cyberspace regulation and Internet governance* (TAS '24, September 16–18, 2024, Austin, TX, USA) Available from: <https://dl.acm.org/doi/pdf/10.1145/3686038.3686049> [Accessed 5 November 2025.]

¹⁰⁶ Deirdre Ahern, (2025) *The New Anticipatory Governance Culture for Innovation: Regulatory Foresight, Regulatory Experimentation and Regulatory Learning*. *European Business Organisation Law Review*.

¹⁰⁷ EASA. (2025) *EASA steps up regulatory framework for Innovative Air Mobility*. [press release] Available from: <https://www.easa.europa.eu/en/newsroom-and-events/news/easa-steps-regulatory-framework-innovative-air-mobility> [Accessed 6 November 2025].

autonomous aviation.¹⁰⁸ By examining these developments, this section demonstrates how comparative regulatory experiences can inform the UAE's efforts to create a governance model that is technologically adaptive, legally coherent and aligned with international best practices.

6.1. EUROPEAN UNION: INTEGRATING DATA PROTECTION, CYBERSECURITY AND AI OVERSIGHT

The EU offers important insights for eVTOL integration as the most well-coordinated model of digital and aviation regulation. The GDPR provides comprehensive safeguards for personal data processing, especially for sensitive categories of data such as biometric and geolocation.¹⁰⁹ Additionally, the EASA incorporates cybersecurity and data assurance principles within its Special Condition for VTOL (SC-VTOL), linking technical reliability to regulatory compliance.¹¹⁰ The EU Artificial Intelligence Act 2024 classifies "AI systems used in the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity as high-risk."¹¹¹ Although autonomous flight control and air traffic systems are not specifically mentioned, their operational similarity to other critical infrastructure categories suggests that they would likely be subject to similar risk governance obligations. These high-risk AI systems are subject to detailed requirements concerning risk management, transparency, human oversight and robustness under Articles 9 to 15 of the Act.¹¹² Overall, these instruments illustrate how the EU's layered regulatory model which combines cybersecurity, data protection and AI accountability, improves systematic governance and provides a coherent framework that the UAE may draw structural inspiration while maintaining regulatory agility.

¹⁰⁸ Alex Engler. (2023) *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*. Brookings. Available from: <https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/> [Accessed 6 November 2025]; Jozef Andraško and others, 'Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union' (2021) 13 Sustainability 1, 21.

¹⁰⁹ *General Data Protection Regulation 2018*, arts. 4(1) & 9.

¹¹⁰ EASA. (2021) *Means of Compliance with the Special Condition VTOL* Available from: https://www.easa.europa.eu/sites/default/files/dfu/moc_sc_vtol_issue_2_12-may-2021_shaded_0.pdf [Accessed 6 November 2025.]

¹¹¹ *EU Artificial Intelligence Act 2024*, art. 6(2) read with Annex III (2).

¹¹² *EU Artificial Intelligence Act 2024*, arts. 9-15.

6.2. UNITED STATES OF AMERICA: EXPERIMENTAL AND DECENTRALISED GOVERNANCE

The USA takes a more experimental and decentralised approach, combining sectoral oversight with innovation-driven testing programs. Through collaborative pilot projects, NASA's Advanced Air Mobility National Campaign and the Federal Aviation Administration's Urban Air Mobility Concept of Operations 2.0 assist in simplifying the technical and operational integration of eVTOLs.¹¹³ Yet, privacy and data governance remain fragmented, i.e., no comprehensive data protection law exists and oversight is divided between sectoral agencies and state-level instruments such as the California Consumer Protection Act.¹¹⁴ The National Institute of Standards and Technology (NIST) issues voluntary cybersecurity and AI risk management frameworks that guide sectoral compliance but do not mandate it.¹¹⁵ Although it encourages innovation, this adaptive model diffuses accountability. For the UAE, the USA experience underscores the importance of regulatory flexibility while illustrating the risks of excessive reliance on voluntary norms in safety-critical domains.

6.3. UNITED ARAB EMIRATES: FOUNDATION AND FUTURE DIRECTION

The UAE's data governance framework for eVTOL systems remains at a formative stage. The UAE PDPL offers a rights-based foundation consistent with international standards but it lacks interpretation or enforcement mechanisms unique to the aviation industry. The GCAA advisories and the UAE Cybersecurity Strategy acknowledge transportation as vital infrastructure but refrain from enforcing binding, industry-specific technical standards.¹¹⁶ As Dubai advances its autonomous air mobility roadmap, the main challenge lies in converting strategic ambition into detailed operational

¹¹³ David Zahn & others, (2023) *NASA Advanced Air Mobility (AAM) Project National Campaign Development of Airspace Operations, Infrastructure and Data* (20230011793) Available from: https://ntrs.nasa.gov/api/citations/20230011793/downloads/NC-069-001%20v2_FINAL_DZ.pdf [Accessed 6 November 2025]; Federal Aviation Administration, *Urban Air Mobility Concept of Operations 2.0* (2023) Available from: <https://www.faa.gov/sites/faa.gov/files/Urban-Air-Mobility-Concept-of-Operations-2.0.pdf> [Accessed 6 November 2025.]

¹¹⁴ Elias Aidun, (2025) *Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations*. 93 *University of Cincinnati Law Review*; Jacob Nix & Pascal A. Bizarro. (2020) *US Data Privacy Law: A Disparate Landscape in Need of Consolidation*. 5 *ISACA Journal*.

¹¹⁵ Mohammed Mustafa Khan. (2023) *NIST Cybersecurity Framework*. 10 *Journal of Scientific and Engineering Research*. 150, 151

¹¹⁶ General Civil Aviation Authority, (2023) *GCAA National Civil Aviation Cybersecurity Strategy* (GCAA-NCACSS) Available from: <https://www.gcaa.gov.ae/en/epublication/Shared%20Documents/GCAA%20National%20Civil%20Aviation%20Cybersecurity%20Strategy-V1-Jun-2023.pdf> [Accessed 6 November 2025.]

regulation. The UAE's efficient collaborative coordination abilities could be leveraged to develop an integrated governance model connecting data protection, AI oversight and aviation safety. This model would draw inspiration from the USA's adaptive experimentation and the EU's structural coherence to build a pragmatic, future-oriented framework.

7. TOWARDS A REGULATORY MODEL FOR EVTOL GOVERNANCE IN THE UAE

The preceding analysis has identified where the UAE's existing frameworks fall short of the demand a new technology such as eVTOL operations will place on them. This section proposes a four-part model addressing those limitations.

7.1. AVIATION SPECIFIC DATA CLASSIFICATION

The UAE Data Office and the GCAA should collaborate to develop a classification standard that separates safety critical operational data from personal data. This may be done using a functional rather than categorical approach. The data set is considered hybrid when the same record is used for both safety and passenger identification purposes, for example biometric boarding logs that function as access control records. Hybrid datasets should be classified under the UAE PDPL's sensitive personal data protections while purely operational telemetry should remain governed by airworthiness rules.

7.2. OPERATIONALISING EXISTING AUTOMATED DECISION SAFEGUARD

Article 18(4) of the UAE PDPL¹¹⁷ requires the controller to include a human element when reviewing automated processing decisions at the data subject's request, furthermore, Article 21¹¹⁸ stipulates a data protection impact assessment wherever automated processing has a legal or serious impact on the data subject, this stipulation shall be clearly met with situations such as emergency rerouting and boarding denial decisions in the case of eVTOLs. Therefore, the limitation is not an absence of statutory right but rather of operational content because neither Article establishes a timeline for review, a threshold for legal and serious impact in the context of aviation or a reporting obligation sufficient to render such review meaningful. It is proposed that the GCAA certification be made conditional upon the operator's ability to ensure compliance with each of these particulars.

¹¹⁷ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 18(4).

¹¹⁸ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 21.

7.3. COORDINATED PROCEDURAL PATHWAY

According to Article 24 of the UAE PDPL,¹¹⁹ the data subject has a right to complain to the Bureau, however, this mechanism does not extend to the GCAA's airworthiness jurisdiction nor to cybersecurity oversight presently divided between the UAE Cybersecurity Office, the Telecommunications and Digital Government Regulatory Authority (TDRA) and the Dubai Electronic Security Center (DESC). Since an eVTOL incident may plausibly involve all three domains simultaneously, a joint coordination function, comprising representation from each body, should be established to prioritise such complaints and direct them to whichever forum that possesses the substantive competence.

7.4. MANDATORY CYBERSECURITY CERTIFICATION

Article 20 of the UAE PDPL requires Controllers to adopt measures consistent with 'international best practices and standards',¹²⁰ but this obligation is not enforced through a sector-specific certification regime, rather it is generic in nature. A comparable concern has already been addressed automotive industry, where cybersecurity certification was earlier optional but is now required as a prerequisite for type-approval from July 2024 according to UNECE's UN regulation No. 155.¹²¹ Drawing on this precedent the GCAA's National Civil Aviation Cybersecurity Guidelines should be converted from voluntary advisory to mandatory precondition for certification for eVTOL deployment.

Taken together, these measures would convert rights and obligations the UAE PDPL confers but does not yet operationalise for aviation, into enforceable, sector-specific practice, without requiring the establishment of a new legal framework.

¹¹⁹ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 24.

¹²⁰ Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data, art 20.

¹²¹ UNECE. (2022) *Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*. UNECE. Available from: <https://unece.org/sites/default/files/2023-01/R155am1e.pdf> [Accessed 26 August 2026].

8. CONCLUSION

Electric vertical take-off and landing systems redefine aviation as an ecosystem mediated by algorithms and driven by data. Their operation relies on the continuous exchange of telemetry, geolocation and biometric data, resulting in crossovers between data protection, aviation safety and AI regulation that existing legal frameworks were not designed to accommodate. In the UAE, these intersections indicate a gap between principle and practice rather than a lack of legislation. The challenge lies in converting the normative foundations of the UAE PDPL, the National Cybersecurity Strategy and the GCAA's advisory circulars into enforceable standards that are appropriate for the complexity of eVTOL operations.

Adopting a doctrinal approach informed by comparative insights, this article contributes to emerging scholarship on data governance in next-generation air mobility by placing the UAE's evolving framework within a global regulatory discourse. By combining data protection, cybersecurity and AI accountability through the GDPR, the EASA's certification framework and the recently passed Artificial Intelligence Act, the European Union is a prime example of structural coherence. The USA demonstrates the benefits of experimental, decentralised governance by combining public-private corporations with regulatory testbeds. Together, these models demonstrate alternative pathways for balancing innovation with legal certainty. One jurisdiction does it with comprehensive regulation while the other with adaptive experimentation.

For the UAE, the synthesis of these trajectories culminates in the four-part regulatory model set out in the previous section. It transforms the rights and obligations that the UAE PDPL already grants but does not yet operationalise for the aviation sector. Each priority addresses a specific limitation identified earlier in the article while employing statutory provisions already present within the UAE PDPL instead of necessitating total amendment of an unfamiliar regulatory model.

The UAE's regulatory flexibility puts it in a position to pioneer a model of adaptive integrity-based governance for urban air mobility, one that links technological ambition with legal oversight. By adopting the model proposed above, the UAE can transform eVTOL regulation from a reactive practice to a proactive instrument of trust and legitimacy. In doing so, it would not only manage emerging risks but also set a standard for responsible innovation in the global evolution of autonomous flying.

LIST OF REFERENCES

- [1] Abeyratne, R. (2024) Advanced Air Mobility: Transcending the Frontiers of Aviation Law. *Frontiers in Law*, 90, 91.
- [2] Abouahmed, A., Kandeel, M. and Zakaria, A. (2024) Personal Data Protection In The United Arab Emirates and the European Union Regulations. *Journal of Governance & Regulation*, 195, 196.
- [3] Abu-Matar, M. and Davies, J. Data Driven Reference Architecture for Smart City Ecosystems (17 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, San Francisco, USA) Available from: <https://ieeexplore.ieee.org/abstract/document/8397556> [Accessed 3 November 2025.]
- [4] Ahern, D. (2025) The New Anticipatory Governance Culture for Innovation: Regulatory Foresight, Regulatory Experimentation and Regulatory Learning. *European Business Organisation Law Review*.
- [5] Al Khateri, M. and Al Zitawi, D. (2025) Cybersecurity and Protection of Digital Data Privacy in the UAE in the Age of Digital Transformation and Artificial Intelligence. *International Journal of Academic Research in Business & Social Sciences*, 491, 498.
- [6] Al-Fahim, A. and Al-Zaabi, F. (2024) *Artificial Intelligence in Law and Ethics in the United Arab Emirates: Balancing Innovation, Regulation, and Cultural Values*. Future Publishing House.
- [7] Al-Rubaye, S. et al. (2023) Advanced Air Mobility Operation and Infrastructure for Sustainable Connected eVTOL Vehicle. *7 Drones* 1, 2.
- [8] Alqahtani, H. and Kumar, G. (21024) *Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems*. 29 Engineering Applications of Artificial Intelligence.
- [9] Alshabibi, M. et al. (2024) *Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review*. 13 Computers 1, 3.
- [10] Andraško, J. et al. (2021) *Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union*. 13 Sustainability 1, 21.
- [11] Andritsos, K. et al. (2022) What is in a Name: Defining Key Terms in Urban Air Mobility. *Journal of Intelligent & Robotic Systems*.
- [12] Aposporis, P. (2024) *A review of global and regional frameworks for the integration of an unmanned aircraft system in air traffic management*. 24 Transportation Research Interdisciplinary Perspectives 1, 11.
- [13] Arafat, M. and Pan, S. (2024) *Urban Air Mobility Communications and Networking: Recent Advances, Techniques, and Challenges*. 8 Drones 1, 12.

- [14] Beduschi, A. (2024) Synthetic data protection: Towards a paradigm change in data regulation? 11 *Big Data & Society*.
- [15] Biswas, K. et al. (2023). Urban Air Mobility: An IoT Perspective. *IEEE Internet of Things Magazine*, 122, 123.
- [16] Brakye, K. and Adam, A. (2025) Cybersecurity Risk Disclosure and Regulatory Compliance: Evaluating Market Sensitivity and Disclosure Effectiveness in U.S. Public Companies EPRA *International Journal of Economics, Business and Management Studies*.
- [17] Brown, N. et al. (2024) Visual and Inertial Datasets for an eVTOL Aircraft Approach and Landing Scenario. 20230016377.
- [18] Castaldo, F. et al. (2024) *Urban Air Mobility: Organisation and Governance of a Frontier Ecosystem* [online] ResearchGate. Available from: https://www.researchgate.net/publication/382021028_Urban_Air_Mobility_Organisation_and_Governance_of_a_Frontier_Ecosystem [Accessed 28 October 2025.]
- [19] Chebotareva, A. and others, (2023) Personal data protection in the civil aviation industry: Technological challenges and legal efforts. 2526 *Modern Approaches in Engineering and Natural Sciences*.
- [20] Çınar, E. and Tuncal, A. (2023) The Future of UAVs in Urban Air Mobility: Public Perception and Concerns. *Turkish Journal of Unmanned Aerial Vehicles*. 50, 54.
- [21] Coche, E. et al. (2024) Unravelling cross country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 112, 115-117.
- [22] Cohen, A., Shaheen, S. and Farrar, E. (2021) *Urban Air Mobility: History, Ecosystem, Market Potential, and Challenges*. 22 *IEEE Transactions on Intelligent Transportation Systems* 6074.
- [23] Dhirani, L. et al. (2023) *Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review*. 23 *Sensors* 1, 3.
- [24] Doo, J. et al. (2021) *NASA Electric Vertical Takeoff and Landing (eVTOL) Aircraft Technology for Public Services*. White Paper no. 20205000636.
- [25] EASA. (2021) *Means of Compliance with the Special Condition VTOL*. [online] EASA. Available from: https://www.easa.europa.eu/sites/default/files/dfu/moc_sc_vtol_issue_2_12may2021_shaded_0.pdf [Accessed 6 November 2025.]
- [26] EASA. (2024) *EASA Concept Paper: guidance for Level 1 & 2 machine learning applications, 2nd ed.* [online] EASA. Available from: <https://horizon.europa.eu/portal/sites/default/files/2024-06/easa->

- concept-paper-guidance-for-level-1-and-2-machinelearning-applications-2024.pdf [Accessed 29 October 2025]
- [27] EASA. (2025) *EASA steps up regulatory framework for Innovative Air Mobility*. [press release] Available from: <https://www.easa.europa.eu/en/newsroom-and-events/news/easa-steps-regulatory-framework-innovative-air-mobility> [Accessed 6 November 2025].
- [28] Ekström, E. (2025) *Cybersecurity Challenges to Airlines: A Literature Review of Risk & Compliance*. Bachelors thesis, Lund University.
- [29] Engler, A. (2023) *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*. [online] Brookings. Available from: <https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparisonand-steps-to-alignment/> [Accessed 6 November 2025]
- [30] EU Artificial Intelligence Act 2024
- [31] *Commission Implementing Regulation (EU) 2023/203*. SI. European Commission. In: EUR-Lex.
- [32] European Commission. (2025) *Data Act Explained*. [online] Europa.eu. Available from: <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained> [Accessed 3 November 2025].
- [33] Farooqui, M. (2025) Rooftop Runways: Evaluating the UAE's Regulatory Framework for Vertiports in Urban Air Mobility. *Via Inveniendi Et Iudicandi*. 149, 153.
- [34] Federal Aviation Administration. (2020) FAA Cybersecurity Strategy. [online] Available from: <https://www.faa.gov/about/plansreports/faa-cybersecurity-strategy> [Accessed 27 August 2025].
- [35] Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data.
- [36] Fleisher, W. et al. (2025) Responsibility and Accountability in an Algorithmic Society. *Philosophy & Technology*.
- [37] Freeman, K. et al. (2021) *Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments*. White paper no. 20205011059.
- [38] General Civil Aviation Authority. (2025) GCAA National Aviation Cybersecurity. [online] Available from: <https://www.gcaa.gov.ae/en/epublication/Pages/gcaacyber-security.aspx> [Accessed 23 October 2025].
- [39] General Data Protection Regulation 2018.

- [40] Golson, J. (2015) *Why We Don't Need Real-Time Flight Tracking*. Wired. Available from: <https://www.wired.com/2015/01/why-we-dont-need-realtime-flight-tracking/> [Accessed 8 September 2025].
- [41] Gritsenko, D. and Wood, M. (2020) Algorithmic governance: A modes of governance approach. *Regulation and Governance*.
- [42] He, J. and Zhang, Z. (2025) *Algorithm Power and Legal Boundaries: Rights Conflicts and Governance Responses in the Era of Artificial Intelligence*. 14 *Laws* 1, 19.
- [43] Hu, L. et al. (2025). *Development and challenges of autonomous electric vertical take-off and landing aircraft*. 11 *Heliyon* 1, 2.
- [44] Human, S. (2022) *Advanced Data Protection Control (ADPC): An Interdisciplinary Overview*. [online] arXiv. Available from: <https://arxiv.org/abs/2209.09724> [Accessed 30 October 2025]
- [45] ISO. (2022) *ISO/IEC 27001:2022*. [online] ISO.org. Available from: <https://www.iso.org/standard/27001> [Accessed 7 October 2025].
- [46] Johnson, R. et al. (2022) Technology Adoption and Acceptance of Urban Air Mobility Systems: Identifying Public Perceptions and Integration Factors. *The International Journal of Aerospace Psychology*, 240.
- [47] Kabashkin, I. and Susanin, V. (2024) *Unified Ecosystem for Data Sharing and AI-Driven Predictive Maintenance in Aviation*. 13 *Computers*.
- [48] Kapil, G. (2025) Cybersecurity Challenges in Aviation. *European Journal of Advances in Engineering and Technology*.
- [49] Karagiannis, C. and Vergidis, K. (2021) *Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal*. 12 *Information* 1, 6.
- [50] Khan, N. and Efthymiou, M. (2021) The use of biometric technology at airports: The case of customs and border protection (CBP). 1 *International Journal of Information Management Data Insights*.
- [51] Khan, S. et al. (2021) On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *Computer Science*, 1, 11.
- [52] Königs, P. (2022) Government Surveillance, Privacy, and Legitimacy. 35 *Philosophy & Technology*.
- [53] Koumoutsidi, A., Pagoni, I. and Polydoropoulou, A. (2022) *A New Mobility Era: Stakeholders' Insights regarding Urban Air Mobility*. 14 *Sustainability* 1, 3.
- [54] Küçük, E. et al. (2025) Solidarity at the intersection of data sharing and data protection: A normative analysis. *Maastricht Journal of European and Comparative Law*.

- [55] Kumar, G. and Altalbe, A. (2024) *Artificial intelligence (AI) advancements for transportation security: in depth insights into electric and aerial vehicle systems*. *Environment, Development and Sustainability* 1, 8.
- [56] Li, T. et al. (2024) *An Innovation Management Approach for Electric Vertical Take-Off and Landing*. 16 *Sustainability* 1,3
- [57] Lu, Y. et al. (2025) *Urban Air Mobility Vertiports: A Bibliometric Analysis of Applications, Challenges, and Emerging Directions*. *Applied Sciences* 1, 18.
- [58] Mascio P, et al. (2025) *Vertiports: The Infrastructure Backbone of Advanced Air Mobility — A Review*. 6 *Eng* 1, 2
- [59] Matheson, R. (2018) *The privacy risks of compiling mobility data*. [online] MIT News. Available from: <https://news.mit.edu/2018/privacy-risks-mobility-data-1207> [Accessed 9 September 2025].
- [60] Matthew, A. (2024) *Cloud Data Sovereignty Governance and Risk Implications of Cross-Border Cloud Storage*. [online] ISACA. Available from: <https://www.isaca.org/resources/news-andtrends/industry-news/2024/cloud-data-sovereignty-governance-andrisk-implications-of-cross-border-cloud-storage> [Accessed 26 August 2025].
- [61] Mendes de Leon, P. and Scott, B. (2023) *Scanning the Air Transport Market in Europe and Beyond: The Position of Airlines and the Evolution of Technical Innovations*. In: Alan D. Meneghetti & Philip Perrotta (eds). *International Comparative Legal Guides*. 15, 17.
- [62] Mishra, S. and Palanisamy, P. (2023) *Autonomous Advanced Aerial Mobility—An End-to-End Autonomy Framework for UAVs and Beyond*. 11 *IEEE Access* 318, 320.
- [63] Mitchell, A. and Riedel, R. (2022) *Building digital platforms to enable advanced air mobility*. [online] McKinsey & Company. Available from: <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/building-digital-platformsto-enable-advanced-air-mobility> [Accessed 23 October 2025].
- [64] Mitici, M. et al. (2024) *Predictive Maintenance Planning for Batteries of Electric Take-Off and Landing (eVTOL) Aircraft Using State-of-Health Prognostics*. *European Safety and Reliability Conference*.
- [65] Mizrak, F. and Akkartal, G. (2024) *Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology*. 10 *Heliyon* 1, 5.
- [66] Mokander, J. et al. (2021) *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations*. *Science and Engineering Ethics* 1, 16.
- [67] Moraes, T. (2024) *Ethical AI Regulatory Sandboxes: Insights from cyberspace regulation and Internet governance*. *TAS* 24. Available from: <https://dl.a>

- cm.org/doi/pdf/10.1145/3686038.3686049 [Accessed 5 November 2025.]
- [68] Naeem, N. (2025) A collaborative system of systems simulation of urban air mobility. 16 *CEAS Aeronautical Journal*.
 - [69] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework*. [online] nvlpubs.nist.gov. Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [Accessed 26 August 2025].
 - [70] Nobles, C., Burrell, D. and Waller, T. (2022) The Need for A Global Aviation Cybersecurity Defense Policy. *Land Forces Academy Review*.
 - [71] Notari, R. (2025) Autonomy Now?: Is It Time To Start Integrating (Autonomous) Urban Air Mobility Vehicles Into The National Airspace System? *Texas A&M Law Review*, 52, 63
 - [72] Nugraha, R. and Scott, B. (2024) *Flying taxis, air mobility and challenges for Indonesia*. *The Jakarta Post*. [online] Available from: [universiteit.leiden.nl](https://scholarlypublications.universiteit.leiden.nl/access/item%3A3728443/view). Available from: <https://scholarlypublications.universiteit.leiden.nl/access/item%3A3728443/view> [Accessed 17 November 2025.]
 - [73] Pagallo, U and Bassi, E. (2020) The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human Rights, and the Free Movement of Data in the EU (2020) 30 *Minds and Machines*.
 - [74] Park, D. et al. (2021) Data ownership in cloud: legal issues. 1 *International Journal of Forensic Engineering & Management*. 1, 2.
 - [75] Pongsakornsathien, N. et al. (2025) Advances in low-altitude airspace management for uncrewed aircraft and advanced air mobility. 154 *Progress in Aerospace Sciences* 1, 20.
 - [76] Purtova, N. (2018) The law of everything. Broad concept of personal data and future of EU data protection law. 10 *Law, Innovation & Technology*.
 - [77] Ramahi, A., Alfiky A. and Tyson, L. (2025) *Dubai aims to beat the traffic with 2026 Joby air taxi liftoff*. [online] Reuters. Available from: <https://www.reuters.com/world/middle-east/dubai-aims-beat-traffic-with-2026-joby-air-taxi-liftoff-2025-07-01/> [Accessed 26 August 2025].
 - [78] Ravich, T. (2020) On-Demand Aviation: Governance Challenges of Urban Air Mobility ("UAM"). 124 *Penn State Law Review*. 657, 666.
 - [79] Robb, L. et al. (2023) Regulatory overlap: A systematic quantitative literature review. *Regulation and Governance*.
 - [80] Salvini, P. et al. (2023) Human involvement in autonomous decision-making systems. Lessons learned from three case studies in aviation, social care and road vehicles. *Frontiers in Political Science* 1, 13.

- [81] Sarkae, M. et al. (2025) A Data-Driven Approach for Performance Evaluation of Autonomous eVTOLs. 61 *IEEE Transactions on Aerospace and Electronic Systems* 3626, 3627.
- [82] Scott, B. and Kurtpinar, O. (2025) Hoffnungen und Hürden: Regulatorische Herausforderungen für Advanced Air Mobility. *Advanced Air Mobility*, (5.1) and *Advanced Air Mobility*, (5.2).
- [83] Srivastava, S. et al. (2024) Fingerprints, Iris Scans, and the Law: Regulating Biometric Human-Computer Interfaces. 9 *Journal of Information Systems Engineering & Management*. 342, 344
- [84] The UAE Government. (2024) *Cyber safety and digital security*. [online] The UAE Government Portal. Available from: <https://u.ae/en/information-and-services/justicesafety-and-the-law/cyber-safety-and-digital-security> [Accessed 7 October].
- [85] The UAE Government. (2024) *Data protection laws*. [online] The UAE Government Portal. Available from: <https://u.ae/en/about-the-uae/digital-uae/data/dataprotection-laws> [Accessed 7 October 2025].
- [86] Tolba, K. (2024) *UAE GCAA unveils National Civil Aviation Cybersecurity Guidelines*. [online] Aviation Business ME. Available from: <https://www.aviationbusinessme.com/news/gcaa-national-civil-aviation-cybersecurity-guidelines> [Accessed 26 August 2025].
- [87] Trimarchi, A. (2023) *Technological Certainties and Regulatory Doubts: An Overlook at Unmanned Aviation and Urban Air Mobility in Europe*. International Conference on Unmanned Aircraft Systems, Poland, June 2023.
- [88] Ukwandu, E. et al. (2022) *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends*. 13 *Information* 1, 2.
- [89] UNECE. (2022) *Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*. [online] UNECE. Available from: <https://unece.org/sites/default/files/2023-01/R155am1e.pdf> [Accessed 26 August 2026].
- [90] Van Dalsem, W. et al. (2021) *A Data & Reasoning Fabric to Enable Advanced Air Mobility*. White paper no. 20205011320.
- [91] Veneruso, P. et al. (2022) Sensing Requirements and Vision-Aided Navigation Algorithms for Vertical Landing in Good and Low Visibility UAM Scenarios. 14 *Remote Sensing*.

- [92] Veneruso, P. et al. (2025) FMCW Radar-Aided Navigation for Unmanned Aircraft Approach and Landing in AAM Scenarios: System Requirements and Processing Pipeline. 25 *Sensors* 1, 2.
- [93] Vida, G. and Török, A. (2023) Expected effects of accident data recording technology evolution on the identification of accident causes and liability. 15 *European Transport Research Review*. 1, 12.
- [94] Voss, W. (2020) Cross-Border Data Flows, the GDPR, and Data Governance. *Washington International Law Journal*, 485, 489
- [95] Voss, W. (2021) Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems. *Colorado Technology Law Journal*, 377.
- [96] Wachter, S. and Mittelstadt, B. (2019) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*.
- [97] Wang, X. et al. (2024) Beyond surveillance: privacy, ethics, and regulations in face recognition technology. 7 *Front. Big Data* 1, 2.
- [98] Wolters, P. (2024) The Influence of the Data Act on the Shifting Balance between Data Protection and the Free Movement of Data. *European Journal of Law & Technology*.
- [99] Xiang, S. et al. (2024) Autonomous eVTOL: A summary of researches and challenges. 3 *Green Energy and Intelligent Transportation*. 1, 13.
- [100] Yashoda, G. et al. (2025) Predictive Maintenance of Aircraft Engine Failure. 5 *International Journal of Advanced Multidisciplinary Research and Studies*.
- [101] Yip, L. (2024) *Comprehensive Multi-Disciplinary Design of an Electric Vertical Take-off and Landing Aircraft*. PhD Thesis, Nanyang Technical University, Singapore, 1, 23.
- [102] Yousef, Z. (2024) How Can the Law Address the Effects of Algorithmic Bias in the Healthcare Context? *LSE Law Review*.
- [103] Zahn, D. et al. (2023) *NASA Advanced Air Mobility (AAM) Project National Campaign Development of Airspace Operations, Infrastructure and Data (20230011793)*. [online] NASA. Available from: https://ntrs.nasa.gov/api/citations/20230011793/downloads/NC-069-001%20v2_FINAL_DZ.pdf [Accessed 6 November 2025]; Federal Aviation Administration, Urban
- [104] Zaidan, E. and Ibrahim, I. (2024) AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanities and Social Sciences Communication*.
- [105] Ziakkas, D. et al. (2025) Designing human-centric intelligent systems in aviation: applications of artificial cognitive systems, AI-enhanced

investigations, and immersive eVTOL simulation training. *Human-Intelligent Systems Integration*.

- [106] Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st Ed. Public Affairs, p. 159.

DOI 10.5817/MUJLT2026-43681

SHUT DOWN, SUED, AND SILENCED: STRATEGIC SUPPRESSION TACTICS OF TECHNOLOGY CORPORATIONS

by

LEE RAUDSEPP * KRISTJAN KIKERPILL †

Technology companies have become defining actors in contemporary democratic societies, wielding structural, instrumental, and discursive power that extends far beyond the marketplace. Yet the full range of strategies through which these companies suppress dissent, neutralise critics, and resist accountability remains largely underexamined. This article addresses that gap by mapping the silencing repertoire of major technology corporations, including those collectively known as GAFAM (Google, Apple, Facebook/Meta, Amazon, and Microsoft), as documented and represented in media reporting. Based on a content analysis of 61 media-reported cases from 2017-2025, we identify how tech companies silence journalists, employees, researchers, competitors, regulators, and democratic institutions. These mechanisms go beyond litigation to include legal intimidation, retaliatory dismissals, regulatory complaints, and legal challenges to legislation. While these actions may appear routine and lawful individually, collectively they create a deliberate suppression system that impacts public discourse and democratic participation. These findings matter less for court decisions than for the effects along the way: deterrence through litigation threats, resource strains on targets, and pressures on governments and regulators. The article adds to debates on platform power, corporate governance, and democratic accountability, emphasizing the need for regulations to counter the silencing influence of tech firms.

* Lee Raudsepp; University of Tartu, Faculty of Social Sciences, Institute of Social Studies; Junior Research Fellow in Information Law; E-mail: lee.raudsepp@ut.ee; ORCID: 0009-0006-1593-7439.

† Kristjan Kikerpill; University of Tartu, Faculty of Social Sciences, Institute of Social Studies; Lecturer in Information Law and Digital Sociology; E-mail: kristjan.kikerpill@ut.ee; ORCID: 0000-0002-1523-3208.

KEY WORDS

strategic silencing, suppression tactics, Big Tech, SLAPP suits, chilling effect, platform power, democratic accountability, corporate governance

1. INTRODUCTION

In the contemporary digital landscape, the technology conglomerates collectively known as GAFAM (Google, Apple, Facebook (Meta), Amazon, and Microsoft) have established unprecedented dominance over global communications, commerce, and information flows.¹ These corporations have evolved beyond traditional market actors to become what scholars describe as entities wielding extraordinary structural and relational power in society.² While heralded for enabling swift innovation, these firms have also come under scrutiny for deploying legal and extra-legal strategies to silence dissent and preserve their expansive power.³

In light of the steadily growing influence of GAFAM, scholars caution that unregulated or under-regulated corporate power can hinder essential checks and balances.⁴ The underlying concern, in essence, is that massive digital platforms, intertwined with everyday life in ways seldom seen before, could erode democratic values by stifling dissent, whether intentionally or as an unintended consequence of risk-averse legal policies. These issues provoke urgent questions about accountability, corporate governance, and the public's right to critique powerful institutions.

This concentration of power has prompted growing scholarly and regulatory attention. This is not merely a question of market size. Khan⁵ argues that the most consequential feature of large platforms is their role as digital infrastructure: other market participants, from retailers to advertisers to application developers, depend on platforms for access to users to such a degree that they routinely avoid conflict, knowing that no viable alternative exists. The result is a structural power that operates quietly,

¹ Cohen, N. (2018) *The Know-it-alls: The Rise of Silicon Valley as a Political Powerhouse and Social Wrecking Ball*. The New Press/Oneworld; Mirrlees, T. (2021) *Getting at GAFAM's 'Power' in Society: A Structural-Relational Framework*. Media, Culture & Society, 43(8), pp. 1–18; Taplin, J. (2017) *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy*. Little, Brown and Company.

² Mirrlees, T. (2021) *Getting at GAFAM's 'Power' in Society: A Structural-Relational Framework*. Media, Culture & Society, 43(8), pp. 3–4.

³ Foer, F. (2017) *World Without Mind: The Existential Threat of Big Tech*. Penguin Press; Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs; Hawley, J. (2021) *The Tyranny of Big Tech*. Regnery Publishing.

⁴ Dickman, C. R. and Danks, M. A. (2012) *Scientists Facing a SLAPP: Frivolous Litigation Stifles Public Comment*. Future Science, p. 61.

⁵ Khan, L. M. (2018) Sources of Tech Platform Power. *Georgetown Law Technology Review*, 2(2), pp. 329–330.

through dependency rather than compulsion, and that extends far beyond the economic domain. Yet while much of that attention has focused on market conduct and competition policy, comparatively little systematic work has examined the full range of strategies through which technology corporations suppress criticism, neutralise opposition, and resist accountability.

Brown and Cefaratti⁶ extend this analysis beyond market conduct, arguing that the same platforms now function as gatekeepers of public discourse, using content moderation, demonetisation, and algorithmic curation to shape what is seen, said, and heard. Where Khan identifies structural power as an economic phenomenon, Brown and Cefaratti treat it as a communicative one: the power to determine whose voice carries and whose does not.

Yet neither economic nor communicative power fully captures the range of strategies through which technology corporations suppress dissent and resist accountability. A significant part of that repertoire is of a legal character, and here the literature on Strategic Lawsuits Against Public Participation (SLAPPs) offers important analytical tools. Canan and Pring⁷ documented how powerful actors deploy civil litigation not to vindicate genuine legal rights, but to shift a public issue out of democratic arenas and into courtrooms, where the costs and demands of defending a lawsuit become the central obstacle to continued participation. Giles and Murphy⁸ develop this point further, arguing that the strategic value of a SLAPP lies precisely in its capacity to succeed without a favourable judgment: a letter from a law firm may be sufficient to cause a critic to withdraw, and the chilling effect on future participation can be achieved without the matter ever reaching a verdict.

This is where the analyses of Canan and Pring and of Giles and Murphy converge on a shared insight, namely that the harm generated by legal suppression is not primarily a function of legal outcomes. Canan and Pring⁹ note that SLAPPs are won by defendants in the vast majority of cases, yet the average duration of proceedings is long enough to achieve the strategic

⁶ Brown, F. and Cefaratti, T. (2019) *Big Tech Tyrants: How Silicon Valley's Stealth Practices Addict Teens, Silence Speech, and Steal Your Privacy*. Post Hill Press/Bombardier Books, pp. 102–103.

⁷ Canan, P. and Pring, G. W. (1988) Strategic Lawsuits Against Public Participation. *Social Problems*, 35(5), pp. 506–519, p. 508.

⁸ Giles, R. and Murphy, B. (2016) SLAPPed: The Use of Strategic Litigation Against Public Participation Suits and Environmental, Social and Governance (ESG) Reporting. *Sustainability Accounting, Management and Policy Journal*, 7(1), pp. 44–79, p. 48.

⁹ Canan, P. and Pring, G. W. (1988) Strategic Lawsuits Against Public Participation. *Social Problems*, 35(5), pp. 506–519, p. 514.

purpose. Giles and Murphy¹⁰ observe that this temporal dynamic is itself the mechanism: the process is the punishment, and the depletion of a critic's time, money, and attention is the objective. The technology sector presents a particularly acute version of this dynamic. The financial asymmetry between a corporation like Google or Meta and an individual journalist, researcher, or civil society organisation is such that even meritless proceedings can impose prohibitive costs on the target.

At the same time, legal suppression is not the whole story. Brown and Cefaratti¹¹ document a range of non-legal silencing mechanisms that technology corporations deploy against internal and external critics alike, including retaliatory dismissals, coordinated lobbying efforts, and the use of platform infrastructure to limit the reach of critical content. These mechanisms rarely appear in isolation. Rather, as Giles and Murphy¹² suggest, legal and communicative strategies tend to function together as part of a broader effort to manage legitimacy, control the terms of public debate, and avoid scrutiny and sanction. The result is a layered and mutually reinforcing system of suppression in which individual actions appear routine and lawful but collectively constitute a deliberate and significant constraint on democratic participation.

This article maps that system. Drawing on a content analysis of media-reported cases from 2017 - 2025 (N=61), we identify and categorise the mechanisms through which major technology corporations seek to silence journalists, employees, researchers, competitors, regulators, and democratic institutions. Our analysis reveals that the range of silencing tactics used by technology companies is wider, more diverse, and more deeply integrated than what current research suggests.

The significance of this finding lies not only in what courts ultimately decide, but in what happens along the way: in the chilling effects generated by the credible threat of litigation, in the resource burdens imposed on those targeted, and in the institutional pressures exerted on governments and regulators. This study, therefore, approaches silencing not as a legal event but as a political and communicative process, one that shapes the boundaries of permissible criticism and participation in the digital age.

¹⁰ Giles, R. and Murphy, B. (2016) SLAPPed: The Use of Strategic Litigation Against Public Participation Suits and Environmental, Social and Governance (ESG) Reporting. *Sustainability Accounting, Management and Policy Journal*, 7(1), pp. 44–79, p. 46.

¹¹ Brown, F. and Cefaratti, T. (2019) *Big Tech Tyrants: How Silicon Valley's Stealth Practices Addict Teens, Silence Speech, and Steal Your Privacy*. Post Hill Press/Bombardier Books, pp. 195–196.

¹² Giles, R. and Murphy, B. (2016) SLAPPed: The Use of Strategic Litigation Against Public Participation Suits and Environmental, Social and Governance (ESG) Reporting. *Sustainability Accounting, Management and Policy Journal*, 7(1), pp. 44–79, p. 50.

The article is structured as follows. The next section reviews existing scholarship on platform power and silencing tactics, establishing the theoretical framework for our analysis. We then outline our methodological approach before presenting our empirical findings. The article concludes with a discussion of the implications of our findings for scholarship on corporate power and democratic accountability.

2. LITERATURE REVIEW

2.1. PLATFORM POWER AND BIGTECH CRITICS

The structural dominance of a small number of technology corporations (primarily GAFAM) over digital infrastructure, communication, and information flows is among the most consequential features of contemporary democratic life. The emergence of GAFAM has fundamentally transformed the global economic and political landscape, creating unprecedented concentrations of power that pose significant threats to democratic governance, market competition, and individual autonomy.¹³ Platform power is defined as the political influence that platform firms achieve when they reach a certain economic scale and build consumer attachment and dependence through tight, intimate connections to their users.¹⁴ Platforms and platformization are thus key components of Big Tech's power.¹⁵

By controlling critical bottlenecks of knowledge, connection, and desire, technology corporations have constituted new forms of private authority that operate at a scale exceeding the regulatory capacity of most nation-states.¹⁶ This dependence is not merely economic: the political power of Big Tech has grown substantially, with technology companies investing billions in lobbying, campaign contributions, and access to opaque avenues for political influence, working to shape regulatory outcomes both domestically and internationally.¹⁷ In 2021 alone, Facebook, Google, Amazon, Microsoft,

¹³ Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *PublicAffairs*

¹⁴ Zuboff, S. (2019) *op. cit.* p. 9; Culpepper, P. D. and Thelen, K. (2020) Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies*, 53(2), pp. 288–290.

¹⁵ Nieborg, D. B. & Helmond, A. (2019). The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance. *Media, Culture & Society*, 41(2), pp. 196–218; Langley, P. & Leyshon, A. (2017). Platform capitalism: The intermediation and capitalisation of digital economic circulation. *Finance and Society*, 3 (1), pp 11–31; Helmond, A. (2015). The platformization of the web: Making web data platform ready. *Social Media + Society*, 1(2), 1–11. Available from: <https://doi.org/10.1177/2056305115603080>; Birch, K. and Bronson, K. (2022) Big Tech. *Science as Culture*, 31(1), pp. 1–14

¹⁶ Srivastava, S. (2023) Algorithmic Governance and the International Politics of Big Tech. *Perspectives on Politics*, 21(3), p. 989.

¹⁷ Okumus, B. (2022) *The Rising Political Power of Silicon Valley*. Issue Brief. Fiker Institute, p. 5.

Apple, Uber, and Twitter spent nearly 70 million dollars lobbying the US government — three times what they had spent a decade earlier.¹⁸

The political dimensions of this authority have been comprehensively theorised. Gerbrandy and Phoa¹⁹ conceptualise the most powerful technology corporations as instances of "modern bigness": A phenomenon where corporations wield instrumental power (lobbying and financing), structural power (setting market terms), and discursive power (shaping normative frameworks). Olesen²⁰ extends this analysis through the concept of "radical indifference": the underlying mechanism of platform capitalism operates independently of content veracity or potential harm, as long as user engagement is maintained, i.e., this indifference arises structurally from the proportional relationship between engagement metrics and profit generation. This indifference, Olesen²¹ argues, constitutes a fundamental threat to democratic deliberation, because democratic systems depend on the distinction between truth and falsehood that the platform logic systematically dissolves.

The communicative architecture through which this power is reproduced has been most comprehensively theorised by Zuboff.²² Surveillance capitalism extracts ever finer-grained behavioural data (including punctuation patterns, photo saturation, posture, and micro-expressions) and uses these for profiling and behavioural prediction. The capital intensity of scaling AI systems at this level means that algorithmic governance is structurally designed to serve the interests of those who already dominate.²³ Zuboff²⁴ characterises the result as "instrumentarian power": an authority that functions by shaping the informational environment in which individual behavior occurs, systematically eroding the conditions essential for personal autonomy and democratic self-governance.

A further structural feature of platform power is opacity. Algorithmic selection rules are far less visible than traditional editorial criteria: source code is proprietary, access to development teams is restricted, and the shift from rule-based to machine-learning algorithms means that the internal decision logic shifts continuously.²⁵ This opacity produces a structural

¹⁸ Okumus, B. (2022) *The Rising Political Power of Silicon Valley*. Issue Brief. Fiker Institute, p. 5.

¹⁹ Gerbrandy, A. and Phoa, B. (2023) *The Power of Big Tech Corporations as Modern Bigness*. In: *Big Tech Corporations and Competition Law*. Routledge, pp. 167–173.

²⁰ Olesen, T. (2025) *Suspicious Organizations: Democracy and the Power of Big Tech*. *Politics & Society*, 54 (1), p. 109.

²¹ Olesen, T. (2025) *op. cit.* p. 109.

²² Zuboff, S. (2019) *op. cit.*

²³ Srivastava, S. (2023) *op. cit.* p. 990.

²⁴ Zuboff, S. (2019) *op. cit.* pp. 221–223.

²⁵ Srivastava, S. (2023) *op. cit.* p. 990.

advantage in accountability disputes: platforms can position themselves as the sole competent enforcement authority over their own systems, displacing public scrutiny with private discretion. Olesen²⁶ frames this through the concept of "democratic disclosure", i.e., the act of bringing organisational misconduct into the public sphere, as the primary mechanism by which journalists, activists, and whistleblowers make platform behaviour visible. The structural barriers to such disclosure are themselves a result of platform power.

2.2.SLAPPS AND ANTI-SLAPP REGULATION

Strategic Lawsuits Against Public Participation (SLAPPs) are among the most directly documented mechanisms by which powerful actors suppress public engagement on matters of public concern. Canan and Pring²⁷ identified the defining feature of SLAPP suits as their purpose: To move a public dispute from democratic forums into courtrooms, where the expense of defending a claim (financial, temporal, and psychological) serves as the main tool of suppression. Giles and Murphy²⁸ make this structural logic explicit: The strategic value of a SLAPP lies in its ability to accomplish its goal without a favorable judgment, since a letter from a law firm may be enough to deter a critic from further public participation.

Canan and Pring²⁹ analysed SLAPPs as a political phenomenon characterised by a three-stage dynamic. A citizen or group raises a concern to a government body or public audience, creating opposition. The opposing party then files civil suits (often for defamation, breach of contract, or interference), and the focus shifts from the public issue to legal proceedings, where the plaintiff's resources and time become decisive.

Canan³⁰ identified four principal motives behind SLAPP filings: retaliation against public opposition, pre-empting future opposition, intimidating defendants and observers, and using litigation as a tool in political or economic conflicts. Canan and Pring³¹ found that defendants prevailed in the large majority of cases that reached a decision, yet the average duration of proceedings was sufficient to achieve the strategic

²⁶ Olesen, T. (2025) *op. cit.* pp. 101–102.

²⁷ Canan, P. and Pring, G. W. (1988) Strategic Lawsuits Against Public Participation. *Social Problems*, 35(5), p. 508.

²⁸ Giles, R. and Murphy, B. (2016) SLAPPed: The Use of Strategic Litigation Against Public Participation Suits and Environmental, Social and Governance (ESG) Reporting. *Sustainability Accounting, Management and Policy Journal*, 7(1), pp. 44–79, p. 48.

²⁹ Canan, P. and Pring, G. W. (1988) *op. cit.* p. 508.

³⁰ Canan, P. (1989) The SLAPP from a Sociological Perspective. *Pace Environmental Law Review*, 7(1), p. 30.

³¹ Canan, P. and Pring, G. W. (1988) *op. cit.* p. 509.

purpose. Giles and Murphy³² articulate the implication precisely: the process is the punishment.

The constitutive elements of a SLAPP suit have been systematically codified in subsequent scholarship. Drawing on Bárd et al.³³, the core characteristics are: the presence of a speaker engaging on a matter of public interest; a chilling effect on both the immediate defendant and observers; a demonstrable intent to intimidate; a vertical power relationship in which the plaintiff holds superior financial and institutional resources; exaggerated damages claims whose function is to maximise the defendant's financial exposure; and meritless claims, i.e., between 70 and 80 percent of SLAPP suits are ultimately dismissed, a fact of little consequence to the plaintiff whose goals are achieved through the proceedings themselves³⁴. Rucz³⁵ confirms that even a successful defence does not neutralise these harms: the financial cost, psychological toll, and time invested in defending a SLAPP proceeding constitute a burden borne by the defendant regardless of the outcome.

The evolution of online participation has further complicated identifying the protected speaker in SLAPP analysis. Canan and Pring's³⁶ original definition referred to persons communicating directly with government bodies, but the European Court of Human Rights in *Steel and Morris v. The United Kingdom*³⁷ established that freedom of expression protections must extend to small and informal groups participating in debates of broad public concern and cannot be reserved for large or formally organised actors. This expanded conception is directly relevant to the technology context, where critics of dominant platforms include individual whistleblowers, academic researchers, civil society organisations, and investigative journalists.

The procedural mechanisms identified above share a common normative function across jurisdictions: to enable defendants to challenge the abusive litigation at the earliest stage possible, thereby trying to displace the economic logic that makes SLAPP suits effective as instruments of suppression, i.e. early dismissal mechanisms, allowing defendants to seek termination of proceedings when the proceedings are manifestly unfounded; reversing the

³² Giles, R. and Murphy, B. (2016) *op. cit.* pp. 44–79, p. 46.

³³ Bárd, P. et al. (2020) *Ad-hoc Request SLAPP in the EU Context (EU-CITZEN Academic Network Study)*. CEPS, pp. 11–13.

³⁴ Bárd, P. et al. (2020) *op. cit.* p. 52.

³⁵ Rucz, M. (2022) SLAPPed by the GDPR: Protecting Public Interest Journalism in the Face of GDPR-based Strategic Litigation Against Public Participation. *Journal of Media Law*, 14(2), p. 383.

³⁶ Canan, P. and Pring, G. W. (1988) *op. cit.*

³⁷ *Steel and Morris v. The United Kingdom* (2005). Application no. 68416/01, ECtHR, 15 February, § 89.

burden of proof etc.³⁸ In response to the growing recognition of SLAPP abuse, legislative frameworks have been developed in a range of jurisdictions: Australia, three Canadian provinces, and 32 US states and the District of Columbia.³⁹ and the European Union adopted the Anti-SLAPP Directive⁴⁰ on 11 April 2024. Anti-SLAPP legislation primarily functions through procedural mechanisms: motions for early dismissal that enable defendants to seek the dismissal of cases at an initial stage; a shift of the burden of proof to the plaintiff to demonstrate the validity of their claim; and costs awards that reduce the financial burden on defendants⁴¹. The purpose of these mechanisms is to distinguish between legitimate exercises of the right of access to courts and abusive instrumentalisation of legal proceedings against public participation.⁴²

Within the European context, the EU Anti-SLAPP Directive represents the most institutionally significant expression of this regulatory approach. It defines the abusive court proceedings against public participation as proceedings that are brought mainly to deter, restrict or punish public participation rather than genuinely enforce a right. Indicators include excessive claims, multiple concurrent proceedings, power imbalances, and intimidation or harassment. Its scope, however, is limited to civil and commercial cases with cross-border implications, meaning that domestic cases fall outside its scope. This is analytically significant, since only 8.5% of the known and documented SLAPP cases across European jurisdictions between 2010 and 2024 would qualify as cross-border cases.⁴³

However, existing anti-SLAPP frameworks have structural limitations in the technology context: standard models presuppose a bounded legal dispute within a single jurisdiction and do not accommodate the transnational, multi-forum litigation campaigns that technology corporations are capable of coordinating across several legal systems simultaneously, nor do they address

³⁸ Kavaliauskaite, J. (2024) Silenced for Participation: A Comparative Analysis of Anti-SLAPP Regulations in the European Union and United States. *Studia Prawno-Ekonomiczne*, 134(2), pp. 10–12; Farrington, F. and Zabrocka, M. (2023) Punishment by Process: The Development of Anti-SLAPP Legislation in the European Union. *ERA Forum*, 24(1), p. 12.

³⁹ Brander, E. and Turk, J. L. (2023) *Centre for Free Expression Releases Report Rating Strength of Anti-SLAPP Laws Around the World*. Business & Human Rights Resource Centre, p. 5.

⁴⁰ Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings (OJ L 2024/1069), *Official Journal of the European Union*, 16 April.

⁴¹ Dickman, C. R. and Danks, M. A. (2012) Scientists Facing a SLAPP: Frivolous Litigation Stifles Public Comment. *Future Science*, p. 64; Kavaliauskaite, J. (2024) *op. cit.* pp. 40–43.

⁴² Farrington, F. and Zabrocka, M. (2023) *Punishment by Process: The Development of Anti-SLAPP Legislation in the European Union*. *ERA Forum*, 24(1), p. 6.

⁴³ Coalition Against SLAPPs in Europe. (2026). *A 2025 report on SLAPPs in Europe: Democracy in the dock*. Available from: <https://www.the-case.eu/resources/2025-report-slapps-in-europe-democracy-in-the-dock/>

the full range of non-litigious silencing mechanisms documented in the cases examined in this study.

2.3. OTHER SILENCING TACTICS

Beyond formal litigation, technology companies deploy a range of silencing mechanisms that do not rely on the courts, but achieve comparable suppressive effects through the employment relationship, contractual architecture, and direct challenges to regulatory authority.

Organisational silencing and employee dismissal represents the most structurally concealed category of suppression, operating entirely within the employment relationship and generally leaving no public legal record. At the heart of this category lies a tension between an employee's democratic right to engage in political speech and the employer's capacity to impose material costs on that participation. In the technology sector, this tension is particularly acute. Technology-employee activism has emerged as a significant governance phenomenon, with workers at companies including Amazon, Google, Microsoft, and Salesforce publicly voicing objections to government contracts, ethical concerns, and social policy decisions; often through open letters, walkouts, and social media, and sometimes at the cost of their employment.⁴⁴ Large technology companies take employee public complaints and "badmouthing" very seriously, as such behaviour can cause reputational damage to the firm and impose higher monitoring costs, creating structural incentives for employers to suppress dissent.⁴⁵ Where employees do raise concerns, retaliatory dismissal is a documented organisational response, and the consequences of dismissal extend beyond the individual targeted: because finding new employment may be considerably harder for someone who has publicly expressed unpopular views, the credible threat of termination is sufficient to deter future speech by those who observe it.⁴⁶

Organisational silencing in the employment context intersects also with a specific EU regulatory framework: the whistleblower directive (2019/1937).⁴⁷ It obliges EU member states to protect reporting persons against retaliation and provides that in case of legal proceedings (incl. those initiated for defamation), they shall not incur liability of any kind as a result of their reports or disclosures. However, as said, this kind of silencing is the most concealed version of suppression.

⁴⁴ Alon-Beck, A. (2020) Times They Are A-Changin': When Tech Employees Revolt! *Maryland Law Review*, 80(1), pp. 120–125.

⁴⁵ Alon-Beck, A. (2020) *op. cit.* pp. 120–125.

⁴⁶ Miller, D. E. (2004) Terminating Employees for Their Political Speech. *Business and Society Review*, 109(2), pp. 232–233.

⁴⁷ Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law. *Official Journal of the European Union*, 23. October. L 305, 17–56.

Strategic litigation against regulatory authority represents another distinct silencing strategy, in which technology corporations deploy legal and political resources against the regulatory frameworks designed to hold them accountable. Challenges to platform transparency legislation (such as requirements that large social media platforms publish reports on content moderation practices) have been framed in the US as First Amendment violations, positioning regulatory compliance as government-mandated speech and the corporation as the bearer of constitutional rights against state overreach.⁴⁸ States themselves can function as amplifiers of platform-based silencing: broadly drafted legal provisions covering extremism, blasphemy, defamation, or "false news" create conditions under which governments pressure platforms to restrict legitimate critical content.⁴⁹

The critical literature reviewed here is not uniform in its politics: Foer's concern is primarily with cultural and intellectual diversity⁵⁰; Zuboff's with autonomy and the conditions of democratic self-governance⁵¹; Taplin's with the creative economy and revenue redistribution⁵²; Cohen's with the gap between Silicon Valley's libertarian self-presentation and its actual social consequences⁵³; Culpepper and Thelen's with the structural conditions of political accountability⁵⁴; Bonini and Treré's with the governance of communicative space and the practical possibilities of resistance.⁵⁵ However, these distinct concerns share a common normative framework: each delineates a mode of governance carried out by private actors that lacks democratic authorization, meaningful procedural accountability, and the legitimacy constraints that public institutions, despite their imperfections, are mandated to uphold.

Bonini and Treré⁵⁶ contend that platforms' governance decisions, such as selecting which content to accept, which accounts to limit in visibility, and which accounts to remove, directly impact the independence of cultural producers. This creates a form of private authority over the communicative space that lacks public accountability. Foer⁵⁷ demonstrates that platforms employ lobbying and influence tactics to preserve their

⁴⁸ Free Press. (2024) *Big Tech Backslide: How the Largest Platforms Are Abandoning Trust and Safety*. Free Press.

⁴⁹ Srivastava, S. (2023) *op. cit.* pp. 989–991.

⁵⁰ Foer, F. (2017) *op. cit.* pp. 11–12.

⁵¹ Zuboff, S. (2019) *op. cit.* pp. 8–9.

⁵² Taplin, J. (2017) *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy*. Little, Brown and Company, pp. 5–6.

⁵³ Cohen, N. (2018) *op. cit.* pp. 53–54.

⁵⁴ Culpepper, P. D. and Thelen, K. (2020) *op. cit.* pp. 288–318, p. 289.

⁵⁵ Bonini, T. and Treré, E. (2024) *op. cit.* pp. 14–15.

⁵⁶ Bonini, T. and Treré, E. (2024) *op. cit.* pp. 14–15.

⁵⁷ Foer, F. (2017) *op. cit.*

structural stance, systematically framing themselves as "neutral platforms" to deny responsibility for the outcomes of their decisions.

Cohen⁵⁸ concludes that at critical junctures, the web was steered by a select group of influential decision-makers toward an individualized, centralized, and commercialized path, despite the original vision of its architects for a decentralized, collaborative platform, and notwithstanding early cautions from Google's founders regarding the distortive impact of commercial search. The moral economy of commercial platforms, as Bonini and Treré⁵⁹ observe, is characterized by a predominantly neoliberal value package: free markets, individualism, data extractivism, performance optimization, and competitive ranking; embedded in the terms of service, enforced through sanctions, and presented as the natural, neutral architecture of digital participation.

This is the context in which the silencing strategies of technology corporations must be understood, considering their structural dominance, communicative gatekeeping, political insulation, and the documented use of economic and legal resources against critics. Platform power, as the collective critical literature shows, is not simply a result of market advantages that competition could dissolve. It is structural, self-reinforcing, and actively protected from democratic challenges. The ways in which technology companies suppress criticism, evade accountability, and resist scrutiny are intrinsic to this structural position: they are manifestations of it. The task now is to identify these mechanisms and evaluate whether current legal frameworks are sufficient to address them.

Building on this theoretical framework, the present study addresses three interrelated concerns. It seeks to map the full range of silencing mechanisms deployed by major technology corporations as documented in media reporting, extending beyond formally recognised SLAPP. It further examines the extent to which these mechanisms share structural characteristics with established SLAPP typologies identified in the existing literature. Finally, it considers what the documented silencing strategies imply for the adequacy of existing legal and regulatory responses, with particular attention to the emerging European framework on anti-SLAPP protection.

⁵⁸ Cohen, N. (2017)*op. cit.* pp. 53–54.

⁵⁹ Bonini, T. and Treré, E. (2024) *Algorithms of Resistance: The Everyday Fight Against Platform Power*. MIT Press, pp. 14–15.

3. DATA AND METHOD

Drawing on a content analysis of media-reported cases from 2017–2025 (N=61), we conducted through systematic searches across multiple search engines (Google, Bing, and Yandex) in order to minimise potential algorithmic bias and ensure comprehensive coverage. These 61 data points refer to 61 distinct media articles, where a single underlying dispute may have generated multiple articles. The unit of analysis is the media representation of a silencing event, not the underlying legal proceeding itself, considering the latter is hard to access. Different articles covering the same underlying dispute at different stages of proceedings, or from different editorial perspectives, were retained as distinct data points, as each contributes independent information about the nature, development, and framing of the silencing tactic in question.

Data collection was conducted through systematic searches across multiple search engines (Google, Bing, and Yandex) to minimize potential algorithmic bias and ensure comprehensive coverage. First search was conducted on Google search engine, and after that other searches were performed as well. This multi-platform approach was particularly crucial given concerns about search result manipulation and the potential for these very corporations to influence the visibility of critical coverage about their practices.

The inclusion of Yandex was considered particularly important given the documented capacity of the very corporations under study to influence the visibility of critical coverage about their own practices through search result manipulation. The search strategy combined targeted keywords designed to capture various forms of legal intimidation and silencing tactics. Primary search terms included "SLAPP," "sued," "silenced," "intimidation," "terminated", and "strategic litigation." Company-specific searches were additionally conducted using terms such as "Google sued," "Microsoft sued," "Apple sued," "Facebook sued," "Meta sued," and "Amazon sued," to ensure comprehensive coverage of legal actions involving each GAFAM entity.

By using this method, we were able to identify recurring patterns, targets, and strategies in discussions about reported incidents and determine if these practices represent a unique form of suppression. Other approaches, like analysing legal cases, wouldn't have been enough, because these suppression tactics happen outside the lawsuits as well (e.g. firing employees, using regulatory pressure). Likewise, methods that rely on interviews would encounter major obstacles due to the sensitive nature of corporate legal strategies and the uneven power dynamics at play. We considered media analysis especially appropriate because of the global reach and influence of

these technology giants, enabling the collection of their legal strategies across different jurisdictions and contexts. Furthermore, media representation is vital in democratic societies because it acts as a watchdog, influences public understanding of corporate power, and is the main way citizens learn about corporate accountability issues.⁶⁰

Articles were included in the final sample if they met the following criteria:

- Published in English;
- Covered legal actions or intimidation tactics involving GAFAM corporations or broader technology companies;
- Discussed instances of suing or silencing individuals, organisations, or entities and
- Provided sufficient detail about the nature of the legal action or intimidation, i.e. the article identified the types of claimants and targets and the any kind of legal action related to suppressing or silencing counterparties. Articles that mentioned a legal dispute only in passing, without providing information sufficient to classify the type of action, were excluded during the process.

Notably, the explicit use of the term "SLAPP" or "silence" was not required for inclusion, as preliminary research indicated that mainstream media outlets rarely employ this technical legal terminology. Instead, articles were selected based on their description of behaviours consistent with SLAPP characteristics, such as lawsuits that appeared designed to silence criticism rather than seek legitimate legal redress.

The study focused on articles published between 2017 and 2025, a period encompassing significant developments in Big Tech's market dominance and increasing scrutiny of its business practices. This timeframe captures the post-2016 period, when concerns about technology companies' influence on democratic processes intensified, through to the present, when regulatory responses have begun to emerge globally.

Following the initial search process, articles that were identical word-for-word across different platforms were systematically excluded to prevent duplication and maintain data integrity. This exclusion criterion was essential given the prevalence of syndicated content and republished articles across various news outlets. No minimum length requirement was imposed on articles, as even brief news reports could contain valuable information

⁶⁰ Christians, C. G. et al. (2017) *Normative Theories of the Media: Journalism in Democratic Societies*. University of Illinois Press, p. 184.

about legal tactics or their effects. However, articles that merely mentioned lawsuits in passing without providing substantive information about the nature of the legal action were excluded during screening.

A custom coding scheme was developed to categorise content based on key features of SLAPPs identified in the literature⁶¹, supplemented by variables capturing elements specific to technology corporations' silencing tactics — including the use of arbitration clauses, non-disclosure agreements (NDAs), employee dismissals, and regulatory pressure.

The coding scheme captured the following variables:

- Legal basis of the action (defamation, breach of NDA, regulatory complaint, etc.);
- Type of target (journalist, activist, employee, competitor, state);
- Nature of the action (lawsuit, threat letter, dismissal, regulatory challenge, etc.);
- Presence of a public interest dimension;
- Power asymmetry indicators and
- Framing in the article (e.g., as intimidation, as routine legal defence).

Each text was coded manually and iteratively, with initial open coding followed by axial categorization to identify dominant themes and emerging typologies. Coded data were analysed thematically to identify recurring patterns across cases. Frequency counts were used to track the distribution of key variables (e.g., types of action, legal grounds), while qualitative memo writing supported interpretive analysis of underlying strategies and narratives. Attention was also paid to how the media portrays the legitimacy or abusiveness of the legal actions in question. The integration of media text with structured coding enabled an exploration of how “totally legal” actions are represented, legitimized, or problematized in public discourse. Through this approach, the study reveals how tech companies strategically leverage legal leeway to shape the boundaries of permissible criticism and participation.

It should be noted that the jurisdiction was not systematically coded, as the study focused on silencing mechanisms rather than geographic distribution. Nevertheless, cases span throughout several countries, which reflects the BigTech's global reach.

⁶¹ Canan, P. and Pring, G. W. (1988) *op. cit.*, pp. 506–519; Bárd, P. et al. (2020) *op. cit.*

4. RESULTS AND DISCUSSION

The final sample comprised 61 articles, in which GAFAM corporations were documented as systematically deploying silencing mechanisms against journalists (4), media outlets (4), employees (13), and individuals or entities who criticise them (34). The distribution of cases across corporations was uneven: X (formerly Twitter) emerged as the most frequent plaintiff in the sample (18), followed by Google/Alphabet, Amazon, Meta/Facebook, Apple, and Microsoft. This distribution reflects both the breadth of these corporations' operations and the degree of public scrutiny they attracted during the study period.

The cases documented in the sample span a wide range of targets and mechanisms. Targets included journalists and media organisations, current and former employees, civil society organisations, competitors, governments, and regulatory bodies. This breadth is itself a substantive finding: it indicates that the silencing repertoire of technology corporations is not confined to any single category of critic or any single institutional arena but operates across the full range of actors and contexts in which corporate conduct is subject to scrutiny and challenge.

The analysis identified three principal patterns of silencing behaviour. The first encompasses classical SLAPP mechanisms: the deployment of civil litigation (including defamation claims, breach of contract suits) against journalists, employees, critics, and civil society organisations, with the primary purpose of burdening targets with legal costs and deterring further public participation rather than securing a favourable judgment on the merits.⁶² The second pattern concerns employment-based silencing: the termination of contracts and the use of internal disciplinary mechanisms against employees who raise concerns publicly or participate in protests. The third pattern, and arguably the most structurally significant, involves the strategic use of litigation against regulatory and governmental authority: BigTech has increasingly initiated legal challenges against governments, state legislatures, and regulatory bodies and it's not to defend individual rights in the conventional sense, but to delay, reshape, or pre-empt regulatory frameworks that would constrain their market conduct or operational autonomy.

⁶² Canan, P., & Pring, G. W. (1988). *op. cit.* p. 508; Giles, R., & Murphy, B. (2016). *op. cit.* p. 49.

4.1.LEGAL MECHANISMS: CLASSICAL SILENCING LAWSUITS (SLAPP-S)

The first and most frequently documented category involves the deployment of classical SLAPP characteristics: civil litigation and legal pressure designed to burden targets with procedural costs and deter continued public participation rather than to vindicate genuine legal rights. Monetary damages claims constituted a primary mechanism through which technology companies pursue silencing actions (13), consistent with the established SLAPP element of exaggerated or meritless claims designed to create a chilling effect⁶³.

Vertical power imbalance was present in over half of the sample (45), reinforcing that the SLAPP suit is a tool wielded by actors with superior financial, institutional, or political resources against targets with limited capacity to defend themselves⁶⁴. Evidence of multiple SLAPP-characteristic suits filed against the same party (15) and against others (24) underscores the strategic, repeat-player nature of many plaintiffs, suggesting patterns of sustained litigation campaigns in which lawsuits serve as ongoing pressure on dissenting voices rather than as isolated legal disputes.

Power accumulation (17) and burden and exhaustion (15) emerge as other core elements of classical SLAPP suits. This demonstrates how technology companies leverage their substantial legal resources to create unsustainable financial and temporal costs for critics. The findings demonstrate that technology companies have refined these tactics to exploit the unique vulnerabilities of digital-age critics, who often lack the institutional support and financial resources necessary to sustain prolonged legal battles against well-funded corporate defendants. Intimidation intent (16) also confirms the original Canan & Pring's⁶⁵ theory about chilling effect as a primary SLAPP objective, validating their conceptualization of SLAPPs as mechanisms designed to warn and punish parties for exercising their rights.

The empirical evidence demonstrates that classical SLAPP mechanisms have been successfully adapted to the digital age context, with technology companies employing these tactics with remarkable consistency and sophistication. The focus has shifted from political freedom of expression to navigating legal and democratic processes, for example, in the case of X Corp.

⁶³ Canan, P. and Pring, G. W. (1988) Strategic Lawsuits Against Public Participation. *Social Problems*, 35(5), pp. 506–519; Bárd, P. et al. (2020) *Ad-hoc Request SLAPP in the EU Context*. CEPS.

⁶⁴ Kavaliauskaite, J. (2024) *Silenced for Participation: A Comparative Analysis of Anti-SLAPP Regulations in the European Union and United States*. *Studia Prawno-Ekonomiczne*, 134(2), pp. 31–52.

⁶⁵ Canan, P. and Pring, G. W. (1988) *op. cit.* pp. 506–519.

versus Media Matters for America, initiated in November 2023. Elon Musk's social media company X filed a lawsuit against liberal advocacy group Media Matters for America, saying it manufactured a report to show advertisers' posts alongside neo-Nazi and white nationalist posts in order to "drive advertisers from the platform and destroy X Corp."⁶⁶ The case demonstrates multiple classical SLAPP characteristics, beginning with Musk's public threat to file "a thermonuclear lawsuit". In addition, the strategic nature of this litigation becomes evident through X Corp.'s multi-jurisdictional approach. Cases were subsequently filed by X companies against Media Matters for America in Texas, Dublin, and Singapore, with Musk stating: "Media Matters is an evil propaganda machine. We are suing them in every country that they operate. And we will pursue not just the organisation, but anyone funding that organisation."⁶⁷

4.2.SUING THE REGULATOR: BIGTECH AS A CHALLENGER OF DEMOCRATIC GOVERNANCE

The empirical analysis reveals a qualitative escalation in the silencing strategies deployed by major technology corporations, i.e., one that extends beyond the suppression of individual critics into the direct contestation of democratic governance itself. Rather than merely deploying litigation against journalists, employees, or civil society organisations, technology corporations have begun systematically initiating legal challenges against governmental entities, regulatory agencies, and legislative processes, with the strategic aim of challenging, delaying, or reshaping the regulatory frameworks that govern their conduct. This represents a fundamental reorientation of corporate legal strategy: litigation is deployed not as a mechanism for resolving genuine legal disputes, but as an instrument of regulatory resistance and institutional capture.

The data reveals multiple cases where technology companies position themselves as victims of government overreach, including X suing New York state over social media content moderation⁶⁸; X sued both the Indian

⁶⁶ Ortutay, B. (2023). *Musk's X sues liberal advocacy group Media Matters over its report on ads next to hate groups' posts*. AP News. Available from: <https://apnews.com/article/elon-musk-media-matters-lawsuit-advertising-neonazi-1fe499daa600f513af27ffa68d2e8b91> [Accessed 15 March 2026].

⁶⁷ Phelan, S. (2025). *Media watchdog to seek injunction halting defamation case taken by Elon Musk's X*. The Irish Independent. Available from: <https://www.independent.ie/irish-news/courts/media-watchdog-to-seek-injunction-halting-defamation-case-taken-by-elon-musks-x/a725422092.html>

⁶⁸ De Guzman, C. (2025). *Musk's X sues New York in latest legal battle over content moderation: What to know*. TIME. Available from: <https://time.com/7295402/elon-musk-x-new-york-lawsuit-free-speech-content-moderation/>

government⁶⁹ and the Australian government.⁷⁰ This pattern demonstrates a fundamental inversion of traditional SLAPP dynamics, where powerful corporations now claim to be defending free speech against government censorship.

Technology companies use free speech arguments to resist regulation, framing compliance as censorship. They deploy SLAPP tactics and litigation across jurisdictions to prolong disputes and claim constitutional protection. This creates a paradox of silencing tactics under the guise of defending democracy, undermining SLAPP and constitutional principles. It also fosters regulatory uncertainty, shifting enforcement costs to governments while gaining benefits. By challenging laws in multiple areas, they set precedents that weaken regulation even where they don't litigate.

Amazon's challenge to "prohibit orders from the Washington Department of Labor & Industries to remedy any types of workplace hazards during the company's pending appeal over the citations"⁷¹ reveals how corporations use litigation to suspend regulatory enforcement while appeals proceed, effectively creating regulatory paralysis through procedural manipulation. This strategy transforms regulatory compliance into prolonged legal battles, creating uncertainty and delay that serve corporate interests while claiming procedural rights. Apple's litigation against the British government, where "UK court lifts secrecy veil, confirms Apple is suing British government over 'backdoor' request",⁷² demonstrates how technology companies challenge government surveillance and security requirements through strategic litigation. By framing government security requests as constitutional violations, these corporations effectively position themselves as defenders of privacy rights while resisting legitimate law enforcement and national security requirements.

The systematic nature of these regulatory challenges suggests a coordinated strategy to establish legal precedents that limit regulatory authority over technology platforms. The case involving Google, where the Texas Attorney General Ken Paxton filed his third lawsuit against Google

⁶⁹ Reuters (2025). X sues Modi's government over content removal in new India censorship fight. *The Guardian*. Available from: <https://www.theguardian.com/technology/2025/mar/20/x-india-censorship-lawsuit-modi-musk>

⁷⁰ Aitchison, M. (2024). Elon Musk's X sues the Australian government in 'free speech' battle after its 'world-first' e-Safety Commissioner ordered an 'offensive' post to be taken down. *Daily Mail*. Available from: <https://www.dailymail.co.uk/news/article-13258303/Elon-Musk-Australian-government-eSafety-Commissioner.html>

⁷¹ Ortutay, B. (2023). *op. cit.*

⁷² Martin, A. (2025) UK court lifts secrecy veil, confirms Apple is suing British government over 'backdoor' request. *The Record*. Available from: <https://therecord.media/uk-court-confirms-apple-suing-over-backdoor-request>

"claiming the tech behemoth tracks the locations of Texans without their consent," shows how companies challenge state-level privacy enforcement, creating a patchwork of legal challenges that collectively undermine regulatory coherence and effectiveness. When multiplied across dozens of state and national jurisdictions, each with its own statutory framework and enforcement apparatus, such challenges collectively undermine regulatory coherence and effectiveness, compelling regulatory bodies to expend institutional resources defending the validity of their frameworks rather than enforcing them.

The cases documented in the sample reveal a coordinated, transnational pattern of governmental litigation. X (formerly Twitter) filed suit against New York State over social media content moderation legislation⁷³, against the Indian government over content removal requirements⁷⁴, and against the Australian government following an order by the eSafety Commissioner to remove content deemed harmful.⁷⁵ The cross-jurisdictional character of these actions is itself analytically significant: by challenging analogous regulatory requirements across multiple legal systems simultaneously, technology corporations generate precedential pressure that can undermine regulatory effectiveness beyond the specific jurisdictions in which proceedings are brought and distribute the costs of regulatory resistance across governments whose resources for sustained litigation are finite.

A defining feature of this litigation strategy is its rhetorical framing, understood here not in the technical sense of 'frame analysis' as developed in sociological and communication research, but in the broader sense of a deliberate communicative strategy by which actors (as in BigTech) deploy constitutional and rights-based vocabulary to reframe institutional interests as matters of public principle. By positioning regulatory compliance as censorship and presenting themselves as defenders of constitutional free speech against government overreach, technology corporations effectively invert the normative logic of democratic accountability: the corporation appears as the aggrieved party, and the state as the aggressor. This framing is strategically powerful precisely because it appropriates the vocabulary of democratic rights (freedom of expression, due process, constitutional protection) in the service of institutional interests that are structurally opposed to the democratic values those rights are designed to protect. The paradox is not incidental: it reflects a sophisticated awareness of the rhetorical resources available to well-resourced legal actors operating

⁷³ De Guzman, C. (2025) *op. cit.*

⁷⁴ Reuters (2025). *op. cit.*

⁷⁵ Aitchison, M. (2024) *op. cit.*

within constitutional traditions that afford broad protections to speech and procedural challenge.

Beyond content moderation, the sample documents litigation strategies aimed at suspending regulatory enforcement through procedural means. Amazon's legal challenge seeking to prohibit orders from the Washington Department of Labor and Industries to remedy workplace hazards during the pendency of an appeal⁷⁶ illustrates how corporations transform routine regulatory compliance into prolonged legal proceedings, creating regulatory paralysis through the strategic exploitation of procedural rights. The practical consequence is that regulatory enforcement is effectively suspended for the duration of litigation, a period that, for corporations with substantial legal resources, can be extended almost indefinitely.

Similarly, Apple's litigation against the British government, challenging a requirement to create a technical backdoor for law enforcement access,⁷⁷ demonstrates how corporations frame legitimate government security requirements as constitutional violations, positioning themselves as privacy advocates whilst simultaneously resisting oversight mechanisms that democratic institutions have determined to be in the public interest.

The cumulative effect of this litigation strategy is the redistribution of the costs of regulatory governance: governments are compelled to defend their legislative authority across multiple forums and jurisdictions, whilst the corporations initiating proceedings concentrate the benefits of regulatory delay and uncertainty. This is not merely a competition law or regulatory compliance problem. It represents a structural challenge to the capacity of democratic institutions to govern the conduct of actors whose resources, technical complexity, and transnational reach systematically exceed the institutional capacities of the states responsible for their oversight. The findings thus point toward a conclusion that conventional litigation frameworks are not equipped to address: when the target of (strategic) litigation is not an individual critic but the democratic state itself, the chilling effect operates not on speech but on governance, thus its consequences are correspondingly more far-reaching.

⁷⁶ Hadero, H. (2025) Amazon sues state agency to block release of company records to Bezos-owned Washington Post. *AP*. Available from: <https://apnews.com/article/amazon-sues-washington-state-post-d3437808a375ec95712f74757ee9fe5b>

⁷⁷ Martin, A. (2025) *op. cit.*

5. CONCLUSION

This article set out to map the silencing repertoire of major technology corporations as documented in media reporting, approaching silencing not as a legal event but as a political and communicative process, which shapes the boundaries of permissible criticism and participation in the digital age. Our study found that while SLAPPs remain the most discussed category of silencing, tech companies are also directing this challenge against public institutions and even legislative process itself.

For tech companies' silencing strategies, legal and communicative aspects function together as part of a broader effort to manage legitimacy, control the terms of public debate, and avoid scrutiny and sanction. This produces a layered and mutually reinforcing system of suppression in which individual actions appear routine and lawful, but collectively constitute a deliberate and significant constraint on democratic participation. Given how large tech companies exercise structural power, future studies should further investigate the nuanced nature of tech companies' silencing strategies, i.e., both SLAPPs and SLAPP-adjacent techniques.

LIST OF REFERENCES

- [1] Aitchison, M. (2024) Elon Musk's X sues the Australian government in 'free speech' battle after its 'world-first' e-Safety Commissioner ordered an 'offensive' post to be taken down. Daily Mail. Available from: <https://www.dailymail.co.uk/news/article-13258303/Elon-Musk-Australian-government-eSafety-Commissioner.html> [Accessed 15.03.2026].
- [2] Alon-Beck, A. (2020) Times they are a-changin': when tech employees revolt! *Maryland Law Review*, 80(1), 120–125.
- [3] Bárd, P., Bayer, J., Luk, N. C., & Vosyliute, L. (2020) *Ad-hoc request SLAPP in the EU context (EU-CITZEN Academic Network Study)*. CEPS., p 11-13.
- [4] Birch, K. & Bronson, K. (2022) *Big Tech*. *Science as Culture*, 31(1), 1–14. DOI: 10.1080/09505431.2022.2036118.
- [5] Bonini, T., & Treré, E. (2024) *Algorithms of resistance: The everyday fight against platform power*. MIT Press, pp. 14–15.
- [6] Brander, E., & Turk, J. L. (2023) *Centre for Free Expression releases report rating strength of Anti-SLAPP laws around the world*. Business & Human Rights Resource Centre, p 5.
- [7] Brown, F., & Cefaratti, T. (2019) *Big tech tyrants: How Silicon Valley's stealth practices addict teens, silence speech, and steal your privacy*. Post Hill Press/Bombardier Books, pp. 102-103.

- [8] Canan, P., & Pring, G. W. (1988) *Strategic lawsuits against public participation*. *Social Problems*, 35(5), 506–519.
- [9] Coalition Against SLAPPs in Europe. (2026) A 2025 report on SLAPPs in Europe: Democracy in the dock. Available from: <https://www.the-case.eu/resources/2025-report-slapps-in-europe-democracy-in-the-dock/> [Accessed 29.07.2026].
- [10] Christians, C. G., Glasser, T. L., McQuail, D., Nordenstreng, K., & White, R. A. (2017) *Normative theories of the media: Journalism in democratic societies*. University of Illinois Press, p 184.
- [11] Cohen, N. (2018) *The know-it-alls: The rise of Silicon Valley as a political powerhouse and social wrecking ball*. The New Press/Oneworld.
- [12] Culpepper, P. D., & Thelen, K. (2020) *Are we all Amazon Primed? Consumers and the politics of platform power*. *Comparative Political Studies*, 53(2), 288–318, pp. 288–290.
- [13] De Guzman, C. (2025) Musk's X sues New York in latest legal battle over content moderation: What to know. TIME. Available from: <https://time.com/7295402/elon-musk-x-new-york-lawsuit-free-speech-content-moderation/> [Accessed 15.03.2026].
- [14] Dickman, C. R., & Danks, M. A. (2012) *Scientists facing a SLAPP: Frivolous litigation stifles public comment*. *Future Science*. DOI: 10.7882/FS.2012.038.
- [15] Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation'), OJ L 2024/1069, 16.4.2024.
- [16] European Parliament & Council of the European Union. (2019) Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law. *Official Journal of the European Union*, L 305, 17–56. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937> [Accessed 29.07.2026].
- [17] Farrington, F., & Zabrocka, M. (2023) *Punishment by process: The development of anti-SLAPP legislation in the European Union*. *ERA Forum*, 24(1), p 6.
- [18] Foer, F. (2017) *World without mind: The existential threat of Big Tech*. Penguin Press.
- [19] Gerbrandy, A., & Phoa, B. (2023) *The power of Big Tech corporations as modern bigness*. In *Big Tech Corporations and Competition Law*. Routledge, pp. 167–173.
- [20] Giles, R., & Murphy, B. (2016) *SLAPPed: The use of strategic litigation against public participation suits and environmental, social and governance (ESG) reporting*. *Sustainability Accounting, Management and Policy Journal*, 7(1), 44–79.

- [21] Hadero, H. (2025) Amazon sues state agency to block release of company records to Bezos-owned Washington Post. AP. Available from: <https://apnews.com/article/amazon-sues-washington-state-post-d3437808a375ec95712f74757ee9fe5b> [Accessed 15.03.2026].
- [22] Hawley, J. (2021) *The tyranny of Big Tech*. Regnery Publishing.
- [23] Helmond, A. (2015) *The platformization of the web: Making web data platform ready*. Social Media + Society, 1(2), 1–11. <https://doi.org/10.1177/2056305115603080>
- [24] Kavaliauskaite, J. (2024) *Silenced for participation: A comparative analysis of anti-SLAPP regulations in the European Union and United States*. Studia Prawno-Ekonomiczne, 134(2), p 31-52.
- [25] Khan, L. M. (2018) *Sources of Tech Platform Power*. Georgetown Law Technology Review, 2(2), 325–334.
- [26] Langley, P. & Leyshon, A (2017) *Platform capitalism: The intermediation and capitalisation of digital economic circulation*. Finance and Society, Vol 3 (1), pp 11–31, DOI: 10.2218/finsoc.v3i1.1936.
- [27] Martin, A. (2025) UK court lifts secrecy veil, confirms Apple is suing British government over ‘backdoor’ request. *The Record*. Available from: <https://therecord.media/uk-court-confirms-apple-suing-over-backdoor-request> [Accessed 15.03.2026].
- [28] Miller, D. E. (2004) *Terminating employees for their political speech*. Business and Society Review, 109(2), pp. 232-233.
- [29] Mirrlees, T. (2021) *Getting at GAFAM’s ‘power’ in society: A structural-relational framework*. Media, Culture & Society, 43(8), pp. 1–18.
- [30] Nieborg, D. B. & Helmond, A. (2019) *The political economy of Facebook’s platformization in the mobile ecosystem: Facebook Messenger as a platform instance*. Media, Culture & Society, 41(2), 196–218.
- [31] Okumus, B. (2022) *The rising political power of Silicon Valley*. Issue Brief. Fiker Institute, p 5.
- [32] Olesen, T. (2025) Suspicious organizations: Democracy and the power of Big Tech. *Politics & Society*, 54(1), p. 109.
- [33] Ortutay, B. (2023) *Musk’s X sues liberal advocacy group Media Matters over its report on ads next to hate groups’ posts*. AP News. Available from: <https://apnews.com/article/elon-musk-media-matters-lawsuit-advertising-neonazi-1fe499daa600f513af27ffa68d2e8b91> [Accessed 15.03.2026].
- [34] Phelan, S. (2025) *Media watchdog to seek injunction halting defamation case taken by Elon Musk’s X*. The Irish Independent. Available from: <https://www.independent.ie/irish-news/courts/media-watchdog-to-seek->

- injunction-halting-defamation-case-taken-by-elon-musks-x/a725422092.html [Accessed 15.03.2026].
- [35] Reuters. (2025) X sues Modi's government over content removal in new India censorship fight. *The Guardian*. Available from: <https://www.theguardian.com/technology/2025/mar/20/x-india-censorship-lawsuit-modi-musk> [Accessed 15.03.2026].
- [36] Rucz, M. (2022) *SLAPPED by the GDPR: Protecting public interest journalism in the face of GDPR-based strategic litigation against public participation*. *Journal of Media Law*, 14(2), pp. 383.
- [37] Srivastava S (2023) *Algorithmic Governance and the International Politics of Big Tech*. *Perspectives on Politics*, Vol 21 (3). doi:10.1017/S1537592721003145, pp 989.
- [38] *Steel and Morris v. The United Kingdom*, Application no. 68416/01 (ECtHR, 15 February 2005), § 89.
- [39] Taplin, J. (2017) *Move fast and break things: How Facebook, Google, and Amazon cornered culture and undermined democracy*. Little, Brown and Company.
- [40] Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

MUJLT Official Partner (Czech Republic)

**ROWAN[®]
LEGAL**

ROWAN LEGAL, advokátní kancelář s.r.o
<https://rowan.legal>

Cyberspace 2025 Partners

**ROWAN®
LEGAL**



Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.

Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide*. 2nd ed. Los Angeles: SAGE Publications, pp.145-151.

Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.

Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.

Citation Guide is available from: <https://journals.muni.cz/public/journals/36/download/Citationguide.pdf>

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.

Use of any special forms of formatting, pictures, graphs, etc. should be consulted.

Only automatic footnotes should be used for notes, citations, etc.

Blank lines should be used only to divide chapters (not paragraphs).

First words of paragraphs should not be indented.

Chapters should be numbered in ordinary way – example: “5.2 Partial Conclusions”.

Submissions

Further information available at

<https://journals.muni.cz/mujlt/about>

LIST OF ARTICLES

Matúš Mesarčík: Esports and the Digital Services Act: Functional Classification of Gaming, Tournament and Streaming Services.....153

Sumaiya Firoz Nomani, Mohammad Rababa, Hussain Al-Ahmad, Husameldin Mukhtar, Nasiruddeen Muhammad, Saad Ali Amin, Burkhard Schafer: Data Protection and Cybersecurity Governance for eVTOL Systems in the UAE: Comparative Lessons from the EU and US.....185

Lee Raudsepp, Kristjan Kikerpill: Shut Down, Sued, and Silenced: Strategic Suppression Tactics of Technology Corporations.....221