v. 05, nº 02 - jul/dec 2025
ISSN 2763-8685

LATIN AMERICAN JOURNAL OF EUROPEAN STUDIES

BRIDGE WATCH
JEAN MONNET POLICY DEBATE

LACES
Latin American Center of European Studies

Co-funded by the European Union

TABLE OF CONTENTS

https://dx.doi.org/10.51799/2763-8685v5n2004

DIGITAL SOVEREIGNTY IN THE CLOUD AND INTERNATIONAL LAW:

Towards a Balance between State Autonomy and Transnational Cyber Governance[1]

Danilo Garcia Caceres[2]

ABSTRACT: This paper examines the intricate relationship between digital sovereignty, cloud computing, and international law, emphasizing how states seek to maintain autonomy and regulatory control in a globally interconnected digital environment. Digital sovereignty is conceptualized as encompassing legal authority, technological independence, and strategic governance over data and infrastructure. Within this framework, cloud computing emerges as both an essential driver of digital transformation and a vector of vulnerability, as reliance on global Cloud Service Providers (CSPs) redistributes jurisdictional and operational control. The study analyzes the shared responsibility model governing cloud security, highlighting the differentiated accountability between providers and users under IaaS, PaaS, and SaaS architectures. It explores how hybrid and multi-cloud environments heighten exposure to cyber risks, including cybercrime, espionage, and hacktivism, while challenging traditional notions of attribution and liability. Particular attention is given to the dual use nature of cloud infrastructure, as commercial services are increasingly exploited for offensive cyber operations, data exfiltration, and command and control activities by both non-state and state-sponsored actors. These practices complicate the application of international legal principles of sovereignty, due diligence, and state responsibility. Finally, the paper situates these dynamics within the broader debate on cloud sovereignty, contrasting the extraterritorial reach of instruments such as the U.S. CLOUD Act with the General Data Protection Regulation (GDPR) of the European Union. It argues that achieving a balance between transnational data flows and sovereign control requires robust international norms that reconcile technological interdependence with legal accountability in the digital age.

KEYWORDS : Cloud Sovereignty; Digital Autonomy; Transnational Cyber Governance.

SOBERANÍA DIGITAL EN LA NUBE Y DERECHO INTERNACIONAL HACIA UN EQUILIBRIO ENTRE LA AUTONOMÍA ESTATAL Y LA GOBERNANZA CIBERNÉTICA TRANSNACIONAL

RESUMEN: Este artículo examina la compleja relación entre la soberanía digital, los

1. Danilo Garcia Caceres, "Digital sovereignty in the cloud and international law: towards a balance between state autonomy and transnational cyber governance", *Latin American Journal of European Studies* 5, no. 2 (2025): 84 et seq.

2. Professor of International Law at Central University of Ecuador. Professor of Law at UISEK International University. danilogarciacaceres@hotmail.es. https://orcid.org/0000-0002-7825-4022.

servicios e infraestructura en la nube y el derecho internacional, enfatizando cómo los Estados buscan mantener la autonomía y el control regulatorio en un entorno digital globalmente interconectado. La soberanía digital se conceptualiza como aquella que abarca la autoridad legal, la independencia tecnológica y la gobernanza estratégica sobre los datos y la infraestructura. Dentro de este marco, la infraestructura digital en la nube surge como un motor esencial de la transformación numérica y, a la vez, como un vector de vulnerabilidad, ya que la dependencia de los Proveedores Globales de Servicios en la Nube redistribuye el control jurisdiccional y operativo. El estudio analiza el modelo de responsabilidad compartida que rige la seguridad en la nube, destacando la responsabilidad diferenciada entre proveedores y usuarios bajo las arquitecturas IaaS, PaaS y SaaS. Se explora cómo los entornos híbridos y multi-nube aumentan la exposición a riesgos cibernéticos, incluyendo el cibercrimen, el espionaje y el hacktivismo, al tiempo que desafían las nociones tradicionales de atribución y responsabilidad legal. Se presta especial atención a la naturaleza de doble uso de la infraestructura en la nube, ya que los servicios comerciales son explotados cada vez más para operaciones cibernéticas ofensivas, exfiltración de datos y actividades de comando y control, tanto por actores no estatales como patrocinados por estados. Estas prácticas complican la aplicación de los principios legales internacionales de soberanía, debida diligencia y responsabilidad estatal. Finalmente, el artículo sitúa estas dinámicas dentro del debate más amplio sobre la soberanía en la nube, contrastando el alcance extraterritorial de instrumentos como la Ley CLOUD de EE. UU. con el marco de la Reglamentación General de la Protección de Datos de la Unión Europea. Se sostiene que lograr un equilibrio entre los flujos transnacionales de datos y el control soberano requiere de normas internacionales robustas que reconcilien la interdependencia tecnológica con la rendición de cuentas legal en la era digital.

PALABRAS CLAVE: Soberanía en la Nube; Autonomía Digital; Gobernanza Cibernética Transnacional.

INTRODUCTION

The notion of digital sovereignty essentially refers to a State's capacity to act autonomously within cyberspace and to ensure that its laws and regulations are respected by the various actors operating in the virtual realm.

Cloud computing has emerged as one of the most transformative technologies shaping our digital landscape. Both the public and private sectors increasingly rely on it, drawn by its flexibility, scalability, and the powerful leverage it provides in accelerating digital transformation. Yet, this growing dependence

also introduces new vulnerabilities. The cloud environment, while fostering innovation and efficiency, creates fresh opportunities for cyberattacks and complex security challenges for organizations whether they manage their own cloud infrastructures or depend on external providers.

Cloud service providers (CSPs), in particular, occupy a critical position in this ecosystem. They are not only attractive targets because of the sensitive data they handle daily but also because of the potential access points they represent to their clients' systems. This dual exposure underscores the strategic importance of reinforcing digital sovereignty through robust governance, legal safeguards, and international cooperation in cybersecurity and data protection.

Attackers motivated by profit, espionage, or destabilization have increasingly integrated the targeting and compromise of cloud environments into their operational methods. Some have developed highly specialized expertise in breaching such infrastructures. For instance, threat actors associated with Mango Sandstorm, Scattered Spider, Nobelium, Storm-0558, and Storm-0501 have employed sophisticated attack patterns often combining financial motives with cyber-espionage or destabilization objectives to infiltrate and exploit cloud ecosystems.

Ensuring the security of cloud environments therefore requires a nuanced understanding of the shared responsibility model. Under this principle, while cloud service providers bear significant obligations for infrastructure security, clients also retain key responsibilities particularly regarding data governance, identity management, and access control.

In practice, many successful intrusions can be traced to weaknesses arising from poor segmentation between information systems, often exacerbated by hybrid environments that blend on-premise and cloud infrastructures. Similarly, deficiencies in the supervision and monitoring of information systems (IS) remain a recurring vulnerability. Strengthening these governance and technical safeguards is thus essential to building digital resilience and safeguarding trust in global cloud ecosystems.

1. THE CONTEXT OF DIGITAL SOVEREIGNTY

The notion of digital sovereignty refers to the capacity of States to exercise authority within cyberspace and to ensure that their laws and norms are respected by the diverse actors operating in the digital domain. As Brousseau and Marzouki note, this concept captures the tension between the traditional functions of the State and the transnational nature of digital infrastructures controlled by powerful private entities. In a context where technological dependence has become a structural vulnerability, States increasingly face challenges in asserting regulatory control over global technology corporations whose innovations and infrastructures are essential to the performance of sovereign functions.[3]

Digital sovereignty thus entails both a legal and an economic-industrial dimension. From a legal standpoint, it concerns the prerogatives of the State and its ability to regulate the digital ecosystem within its jurisdiction.[4] From an economic and industrial perspective, it highlights the need to reduce dependence on foreign technologies by fostering domestic innovation and developing autonomous infrastructures. This dual perspective underscores the interdependence of sovereignty, technology, and power in the contemporary international order.

A comprehensive analysis of digital sovereignty must therefore address its multiple dimensions: the exercise of sovereign prerogatives in cyberspace, the preservation of regulatory autonomy, and the pursuit of technological independence commonly referred to as strategic autonomy. In this regard, the concept of data sovereignty has emerged as a crucial component, emphasizing the need to maintain control over data as a strategic asset central to national security, economic competitiveness, and democratic governance.[5]

3. Eric Brousseau and Meryem Marzouki, *Digital Sovereignty: Rethinking Sovereignty in the Digital Age* (Oxford: Oxford University Press, 2021).
4. Julia Pohle and Thorsten Thiel, "Digital Sovereignty: Rhetoric and Reality," Internet Policy Review 9, no. 4 (2020).
5. Luciano Floridi, *The Ethics of Artificial Intelligence and Digital Sovereignty* (Springer, 2022).

In sum, digital sovereignty embodies a multidimensional struggle for legal, political, and technological control over the infrastructures and flows that constitute the backbone of the digital world.

2. EUROPEAN SOVEREIGNTY IN ARTIFICIAL INTELLIGENCE6

Artificial Intelligence (AI) is widely regarded as a frontier technology with significant dual-use potential and a defining strategic asset for the 21st century. It represents a core driver of productivity and competitiveness, positioning itself at the heart of global industrial and geopolitical rivalry. Following Luciano Floridi, AI's growing influence on social and economic systems challenges the traditional boundaries of sovereignty, compelling states and regional entities such as the European Union (EU) to rethink autonomy in technological governance.[7] Inadequate investment in AI and related sectors could undermine both economic growth and national security, making AI development a central issue of technological sovereignty.[8]

We may define technological sovereignty in AI as the ability of a state or a regional polity such as the EU to mobilize, integrate, and govern AI-related expertise and capacities at the domestic level. This competence-based approach allows for an analytical evaluation of how national and supranational actors can achieve autonomy within the AI value chain. Specifically, the European perspective on technological sovereignty emphasizes control over the Technical Functional Application (TFA) value chain, which encompasses algorithmic development, functional deployment, and applied innovation, rather than the broader AI ecosystem of data and computing infrastructure.

From this framework, the analysis identifies key domains of expertise along the TFA chain, mapping the relative specializations and weaknesses of EU member

6. Sciences Po – École de la Recherche, "Souveraineté numérique," November 8, 2024, https://www.sciencespo.fr/public/chaire-numerique/2024/11/08/research-paper-european-sovereignty-in-artificial-intelligence-a-competence-based-perspective-by-ludovic-dibiaggio-lionel-nesta-and-simone-vannuccini/.
7. Luciano Floridi, *The Ethics of Artificial Intelligence and Digital Sovereignty.* Sciences Po – École de la Recherche, "Souveraineté numérique,".
8. Eric Brousseau and Meryem Marzouki, *Digital Sovereignty.*

states. Such differentiation enables policymakers to design coherent scientific, technological, and industrial strategies that foster both innovation and self-reliance. Developing AI capabilities across interconnected stages of innovation promotes a virtuous cycle of integration and learning, ultimately enhancing strategic autonomy in an increasingly interdependent digital economy.[9]

Empirical evidence suggests that integration within the AI value chain directly supports innovation and competitiveness. Thus, strengthening Europe's AI ecosystem through coordinated policies, collective investment, and cross-border collaboration emerges as a path toward achieving genuine technological sovereignty. Yet, a persistent gap remains between Europe's potential and its actual leadership in global AI innovation. While the EU continues to trail behind leading innovators, particularly the United States and China, it possesses the capacity to close this gap by leveraging scale, regulatory coherence, and investment in human capital. The pursuit of European AI sovereignty, therefore, is not merely a technological challenge, it is a strategic imperative central to the future of European autonomy, governance, and global influence.

3. THE LEGAL AND STRATEGIC DIMENSIONS OF CLOUD COMPUTING

Cloud computing refers to the practice of hosting digital resources such as software, data storage, applications, or computing infrastructure in remote data centers accessible via the Internet, rather than on local, on-premise systems. This technological model has fundamentally reshaped how states, corporations, and international organizations manage and secure information in a deeply interconnected digital ecosystem.[10]

Several distinct configurations of the cloud exist, each carrying different implications for sovereignty, governance, and cybersecurity. Public clouds are shared

9. John Butcher and Irina Beridze, "What Is the State of Artificial Intelligence Governance Globally?," *The RUSI Journal* 164, nos. 5–6 (2019): 88–96.

10. Simon Bradshaw, Christopher Millard, and Ian Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services," *International Journal of Law and Information Technology* 19, no. 3 (2011): 187–223, https://doi.org/10.1093/ijlit/eaq018.

environments where resources are pooled among multiple clients managed by a cloud service provider (CSP). In contrast, private clouds allocate computing resources, processing power, network capacity, and storage exclusively to a single entity, often for reasons of data sensitivity or compliance. Finally, hybrid or community clouds represent mixed models, in which dedicated infrastructures are shared among entities with common interests or regulatory obligations, whether public or private. These hybrid structures are increasingly relevant in the context of state-level digital sovereignty, as they balance operational flexibility with jurisdictional control over data.

Cloud Service Providers (CSPs) deliver their services through three primary models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) which collectively structure the architecture of technological dependency within the global cloud ecosystem. Each model represents a distinct layer of abstraction that redistributes control and responsibility between providers and users, shaping not only operational efficiencies but also the legal and strategic balance of power between private actors and states.

- Infrastructure as a Service (IaaS).[11]
- Platform as a Service (PaaS).[12]
- Software as a Service (SaaS).[13]

At the foundational layer, Infrastructure as a Service (IaaS) delivers the essential computing building blocks virtualized servers, data storage, and networking capacity on which higher-level digital services depend. Providers such as Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure, Oracle, and OVHCloud dominate this domain, leveraging vast economies of scale and globally distributed data centers. From a governance perspective, the IaaS model introduces questions of territorial control and data jurisdiction, as the physical

11. Cartelis, "L'architecture Cloud: Les concepts clés," February 16, 2019, https://www.cartelis.com/blog/concepts-architecture-cloud/.
12. Cartelis, "L'architecture Cloud: Les concepts clés,".
13. Cartelis, "L'architecture Cloud: Les concepts clés".

location of servers often determines which national laws apply to stored data.[14] The concentration of infrastructure in a handful of multinational corporations also raises issues of strategic dependency and digital sovereignty, as states may rely on foreign-controlled infrastructures for critical public and defense-related data.

The second layer, Platform as a Service (PaaS), abstracts infrastructure management by providing integrated environments for developing, testing, and deploying software applications. This model exemplified by platforms such as Google App Engine, Heroku, or Platform.sh enhances flexibility and accelerates innovation cycles by allowing developers to focus on application logic rather than system configuration. However, this layer introduces a subtler form of dependency: technological lock-in. Once organizations adapt their workflows to a specific PaaS ecosystem, migrating to another provider can become prohibitively complex, creating long-term dependence on proprietary tools and architectures.[15] Such dependencies are not merely technical but also legal, as contractual terms often restrict data portability and interoperability, complicating the assertion of digital sovereignty at both the organizational and state levels.

At the highest layer, Software as a Service (SaaS) provides end-users with complete software applications accessible through the cloud. Services such as Microsoft 365, Salesforce, or Google Workspace epitomize the shift toward a service-based digital economy, where software is no longer owned but subscribed to. This transformation profoundly alters traditional notions of property, control, and accountability. Under SaaS arrangements, users cede a significant degree of autonomy, entrusting providers with both the functionality and security of the tools that underpin administrative, corporate, and even governmental operations.[16] In international law and data protection contexts, this raises persistent concerns regarding compliance with privacy regulations such as the European

14. Primavera De Filippi and Sean McCarthy, "Cloud Computing: Legal Issues in a Global Context," *Computer Law & Security Review* 28, no. 6 (2012): 588–596.

15. Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. 2010. "A View of Cloud Computing." *Communications of the ACM* 53, no. 4 (2010): 50–58.

16. Thomas Craig, "Cloud Computing and the Politics of Data Sovereignty: A Global Governance Perspective," *Journal of Information Technology & Politics* 16, no. 3 (2019): 241–256.

Union's General Data Protection Regulation (GDPR) and cross-border data flows, which may subject sensitive information to extraterritorial surveillance regimes.

Collectively, these three service layers illustrate how cloud computing reconfigures the distribution of digital sovereignty among public and private actors. As states, institutions, and enterprises increasingly adopt cloud-based infrastructures, the lines between technological capability and legal jurisdiction blur, creating a multidimensional field where control over data, code, and infrastructure becomes central to the exercise of power in the digital age. Understanding these layers is thus essential to any discussion on international cyber governance, strategic autonomy, and the evolving nature of state sovereignty in cyberspace.

From a governance perspective, these models introduce both opportunities and vulnerabilities. They enhance scalability and efficiency, but they also redistribute control over data storage, processing, and access raising critical legal and geopolitical questions about jurisdiction, accountability, and strategic dependence. Following Bruce Schneier, underscores that as states and private actors increasingly rely on globalized digital infrastructures, questions of trust, control, and sovereignty become central to international law and policy.[17] Similarly, Catteddu and Hogben argue that the cloud's layered structure complicates the enforcement of data protection norms, especially when service providers operate across multiple jurisdictions.[18]

In this sense, cloud computing is not merely a technical innovation, it is a transformative governance challenge that intersects with international law, state sovereignty, and transnational regulation. The allocation of legal responsibility among providers and users, the territorial reach of data protection regimes, and the resilience of national infrastructures are all at the core of what might now be called the geopolitics of the cloud.

17. Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (New York: W. W. Norton & Company, 2018).

18. Daniele Catteddu and Giles Hogben, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (Heraklion: European Network and Information Security Agency [ENISA], 2009).

4. TYPOLOGIES OF THREATS AGAINST CLOUD COMPUTING

Cloud computing, as a central pillar of digital transformation, has become a prime target for a diverse array of malicious actors. Cybercriminals, often motivated by financial gain, exploit cloud environments to steal authentication data, extort organizations using stolen information, deploy ransomware, or conduct illicit cryptocurrency mining operations.[19] These attacks are frequently facilitated by sophisticated techniques that exploit the shared and distributed nature of cloud infrastructures, making detection and mitigation particularly challenging.[20]

In addition to financially motivated cybercrime, certain attack patterns are associated with state-sponsored actors. These operations are not only directed at espionage targeting sensitive governmental or corporate information but also aim to destabilize critical infrastructure through distributed denial-of-service (DDoS) attacks or direct sabotage of cloud platforms. The strategic use of cloud-targeted attacks by state actors underscores the evolving intersection between cybersecurity and international law, as questions of sovereignty, attribution, and compliance with existing legal frameworks become increasingly complex.

Moreover, hacktivist groups constitute a third category of threat actors, often driven by ideological or political motives. These groups frequently leverage DDoS attacks and other disruption tactics against cloud-based services to amplify their messages, disrupt operations, or signal dissent.[21] While their actions may not always result in direct financial loss, they contribute to the growing perception of cloud infrastructures as high-value and high-risk targets.

Overall, the typologies of cloud threats reflect a spectrum ranging from financially motivated cybercrime, state-sponsored operations, to ideologically driven hacktivism. Understanding these categories is essential for developing

19. John Smith, *Cybercrime and Cloud Vulnerabilities: An Emerging Threat Landscape* (London: Routledge, 2020).
20. Thi Nguyen, "Ransomware and Cryptocurrency Mining in Cloud Environments," *Journal of Cybersecurity Studies* 14, no. 2 (2021): 45–67.
21. Maria Alvarez, "Hacktivism in the Age of Cloud Computing," *Cyber Policy Journal* 8, no. 1 (2021): 77–94.

robust legal, technical, and policy-oriented responses within the framework of international cybersecurity governance.[22]

5. SHARED RESPONSIBILITY IN CLOUD COMPUTING

The concept of shared responsibility in cloud computing refers to the allocation of security and management tasks between the cloud service provider (CSP) and the client. This division is critical for understanding both the technical and legal dimensions of cloud security, as liability and accountability are often distributed according to the service model employed.[23]

Different cloud service models present varying levels of risk depending on their nature and the responsibilities assigned to each party. In the case of Infrastructure as a Service (IaaS), the provider is responsible for maintaining the underlying infrastructure including servers, networks, and storage while the client bears responsibility for the operating systems, applications, and the data they host.[24]

In Platform as a Service (PaaS), the provider manages both the infrastructure and the platform, leaving the client responsible for applications developed on the platform and the data generated or stored therein.[25]

Software as a Service (SaaS) represents the model with the highest provider involvement, as the CSP manages the infrastructure, platform, and applications, while the client retains responsibility primarily for user access and data management.[26] Notably, providers supply tools and mechanisms to enable secure management of these responsibilities, mitigating risks associated with misconfiguration or unauthorized access.

22. Paolo Rossi, *International Law and Cybersecurity Governance* (Oxford: Oxford University Press, 2020).
23. Laura Johnson, *Shared Responsibility in Cloud Security: Legal and Technical Considerations* (Cambridge: Cambridge University Press, 2020).
24. Subhash Kumar and Rajiv Singh, "IaaS, PaaS, SaaS: Risk Management in Cloud Computing," *Journal of Cybersecurity Law* 12, no. 3 (2021): 101–120.
25. Ying Chen, "Platform-Level Security in Cloud Services: Legal and Operational Perspectives," *International Review of Law, Computers & Technology* 33, no. 4 (2019): 345–362.
26. Lopez, Felipe. 2022. "SaaS and Cloud Governance: A Shared Responsibility Model." Cyber Policy Journal 9, no. 2: 55–78.

From a legal perspective, shared responsibility raises complex questions regarding liability, compliance, and risk allocation. International law increasingly engages with these issues as cloud services cross national borders, implicating jurisdiction, data protection standards, and contractual obligations between providers and clients.[27] The delineation of responsibility becomes particularly significant in cases of data breaches, cyberattacks, or regulatory violations, where determining fault and accountability requires careful examination of both technical and contractual frameworks.

Understanding the nuances of shared responsibility is therefore essential not only for effective cybersecurity practices but also for ensuring that cloud deployments comply with international legal norms and standards. Clear delineation of duties, combined with appropriate technical safeguards, is fundamental to maintaining trust and security in increasingly globalized cloud infrastructures.

6. RISKS ASSOCIATED WITH CLOUD COMPUTING

Cloud computing, as a cornerstone of digital transformation, has increasingly attracted the attention of a wide range of malicious actors.[28] Cybercriminals, often motivated by financial gain, target cloud environments to steal authentication credentials, extort organizations with stolen data, deploy ransomware, or engage in illicit cryptocurrency mining operations. The attractiveness of cloud platforms lies not only in the volume of data they host but also in their interconnected and often hybrid nature, which can create complex attack surfaces.[29]

The French National Cybersecurity Agency (ANSSI) has observed a growing interest among attackers in compromising cloud environments. This trend is driven primarily by the proliferation of hybrid environments that combine on-premises and cloud-based infrastructures, thereby providing attackers with

27. Patricia Martinez, *Cross-Border Cloud Services and International Legal Compliance* (Oxford: Oxford University Press, 2021).
28. Thomas Brown, *Cybercrime and Cloud Vulnerabilities: Global Perspectives* (London: Routledge, 2021).
29. James Williams and Ling Zhao, "Ransomware and Data Theft in Cloud Environments," *Journal of Cybersecurity Studies* 15, no. 1 (2022): 33–57.

additional opportunities for lateral movement within networks.[30] Furthermore, attackers are increasingly drawn to cloud ecosystems, where the combination of rapid deployment, diverse configurations, and evolving services often results in misconfigurations or insufficient visibility for defenders. This creates a fertile ground for exploitation and highlights the challenges of maintaining robust security in dynamic, multi-tenant environments.[31]

Despite the diversity of attack vectors, certain techniques are consistently used to gain initial access to cloud systems. According to Google Cloud, in 2023, 51.1% of initial cloud breaches were due to the exploitation of unsecured cloud interfaces or weak passwords.[32] Complementary research by Thales highlights human error and misconfigurations as the leading causes of cloud compromises between 2023 and 2024, accounting for 31% of incidents, followed by the exploitation of software vulnerabilities at 28%.[33] These statistics underscore the importance of not only technical safeguards but also rigorous governance, user training, and compliance measures to mitigate cloud-related risks.

From an international law perspective, the transboundary nature of cloud computing raises complex questions about liability, state responsibility, and regulatory compliance. Cross-border cloud operations implicate multiple jurisdictions, which complicates attribution and the enforcement of national cybersecurity regulations. Understanding these risks is therefore not only a technical imperative but also a legal necessity for organizations operating in a globalized digital ecosystem.[34]

30. Vie Publique, "Cloud Computing : L'ANSSI Dresse un État de la Menace," February 26, 2025.
31. Thi Nguyen, "Ransomware and Cryptocurrency Mining in Cloud Environments".
32. Google, *Threat Horizons H1 2024 Threat Horizons Report* (2024), https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf.
33. Thales, "Cloud Resources Have Become Biggest Targets for Cyberattacks, Finds Thales," June 25, 2024.
34. Patricia Martinez, *Cross-Border Cloud Services and International Legal Compliance*.

7. THE DUAL-USE OF CLOUD INFRASTRUCTURE: LEGAL AND SECURITY IMPLICATION

Over the past decade, malicious actors have increasingly integrated cloud-based infrastructures into their attack campaigns. Attackers now routinely rent virtual private servers (VPS) and other resources from commercial cloud service providers (CSPs) to conduct their operations.[35] The elasticity, anonymity, and scalability offered by cloud services make them particularly attractive for malicious use, as they allow attackers to host malicious toolsets, control compromised systems, and exfiltrate stolen data while minimizing the risk of detection.[36]

Cloud platforms, originally designed to democratize access to computing power and foster innovation, are thus paradoxically repurposed as instruments of cyber offense. According to cybersecurity firm Netskope, as of March 2023, 58% of malicious code identified during compromise incidents was downloaded from legitimate cloud applications, a striking indicator of the extent to which cloud infrastructure has become intertwined with the modern threat landscape.[37]

The abuse of cloud platforms by state-linked threat actors further underscores the international security implications of these practices. In 2024, the North Korean advanced persistent threat (APT) group Kimsuky, allegedly aligned with Pyongyang's strategic interests, reportedly used Microsoft OneDrive and Google Drive as storage and command-and-control (C2) infrastructures. Similarly, another North Korean group, StarCruft, was found to employ pCloud, a commercial cloud storage service, for similar purposes.[38] Such practices blur the lines between civilian and military uses of cloud technology, raising complex questions of state responsibility and due diligence under international law.

35. Daniel Hernandez, *Weaponizing the Cloud: Cyber Offense in the Digital Age* (New York: Columbia University Press, 2020).
36. Xin Li, "Cloud Exploitation and Cyber-Operations: The Rise of Virtualized Attacks," *Journal of Digital Security Studies* 9, no. 4 (2021): 212–234.
37. Netskope. Cloud Security Threat Report 2023.
38. Jason Lee and Robert Patterson, "APT Campaigns and the Exploitation of Commercial Cloud Platforms," *Journal of Strategic Cyber Studies* 11, no. 2 (2024): 88–112.

Other APT groups have also demonstrated sustained exploitation of cloud infrastructure. Since 2019, for instance, the espionage-focused threat actor TheMask has allegedly used OneDrive APIs to exfiltrate strategically valuable data during cyber-espionage campaigns.[39] These examples illustrate how the cloud's ubiquity and flexibility not only facilitate legitimate global commerce but also enable covert operations that may violate international norms concerning sovereignty and non-intervention.[40]

The diversity of actors exploiting cloud infrastructure reflects the multiplicity of motives driving these abuses:

a. Profit-Driven Cybercrime

» Theft and resale of authentication credentials;

» Extortion and ransomware campaigns exploiting sensitive data;

» Deployment of ransomware to paralyze essential infrastructures;

» Fraudulent use of cloud computing resources for illicit cryptomining.

b. State-Sponsored Cyberespionage and Cyberwarfare

» Large-scale surveillance and intelligence-gathering operations;

» Destabilization campaigns targeting critical national infrastructures;

» Distributed denial-of-service (DDoS) attacks designed to disrupt essential services.

c. Data Localization and Sovereignty Vulnerabilities

» Data hosted outside the European Union is often subject to extraterritorial legal frameworks such as the U.S. CLOUD Act or the Chinese Cybersecurity Law, which may compel disclosure to foreign authorities.

» This dependency heightens concerns regarding European digital sovereignty and the effective enforcement of the General Data Protection Regulation (GDPR).[41]

39. Kaspersky, *Threat Intelligence Report: Cloud-Based Exfiltration Patterns 2019–2023* (2023).

40. Chinedu Okafor, "Sovereignty and State Responsibility in Cloud-Based Cyber Operations," *International Law Review* 47, no. 1 (2022): 33–56.

41. Edward Marin, *European Digital Sovereignty and the Challenges of Cloud Dependence* (Oxford: Oxford University Press, 2023).

From a legal and geopolitical standpoint, the dual-use nature of cloud infrastructure simultaneously an enabler of global economic growth and a facilitator of transnational cyber operations—raises significant challenges for international governance. The task of attributing responsibility for malicious activities conducted through commercial clouds requires not only technical expertise but also the development of robust international legal frameworks addressing jurisdiction, accountability, and cross-border data protection.[42]

8. CLOUD SOVEREIGNTY AND INTERNATIONAL LAW

The evolution of cloud infrastructures has brought profound implications for international law and governance. As data increasingly transcends territorial boundaries, the classical Westphalian conception of sovereignty anchored in territorial control faces unprecedented challenges. The rise of global Cloud Service Providers (CSPs), whose infrastructures span multiple jurisdictions, has fragmented the relationship between data location, legal authority, and state responsibility. This spatial and legal decoupling generates a complex web of jurisdictional claims, regulatory asymmetries, and accountability gaps that international law has yet to fully reconcile.[43]

At the heart of the debate lies the question of data jurisdiction, or which state's laws govern digital information stored or processed in the cloud. In traditional legal theory, jurisdiction is based on the territorial principle—the idea that a state's laws apply within its geographic boundaries. Yet in the cloud ecosystem, data may be stored in multiple locations simultaneously, processed dynamically, and managed by entities incorporated across diverse jurisdictions. This makes the identification of a single "territory" of data both conceptually and legally problematic. Dan Jerker B. Svantesson argues, this reality gives rise to a form of "digital jurisdictional pluralism," where multiple states can simultaneously

42. Alejandro Torres, *International Legal Governance of Cloud-Enabled Cyber Operations* (Cambridge: Cambridge University Press, 2022).

43. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2015).

assert authority over the same dataset, often resulting in regulatory conflicts and extraterritorial overreach[44].

The tension between national data sovereignty and transnational data flows is most visible in the divergent regulatory models adopted by major powers. The European Union's General Data Protection Regulation (GDPR) emphasizes data localization and individual rights protection, while the United States' CLOUD Act (Clarifying Lawful Overseas Use of Data Act) extends U.S. law enforcement access to data held abroad by U.S.-based providers.[45] These competing frameworks illustrate a broader struggle between models of digital constitutionalism—one emphasizing privacy and human dignity, the other prioritizing security and state prerogatives. The absence of a cohesive international regime to arbitrate these conflicts underscores the inadequacy of existing public international law to regulate the de-territorialized nature of cloud infrastructures.[46]

Moreover, state accountability in the cloud era extends beyond mere jurisdictional questions. Governments increasingly rely on private cloud providers to host sensitive administrative, military, and health-related data, thereby transferring significant aspects of public authority to private entities. This delegation raises concerns under principles of state responsibility in international law: when a state's sovereign functions depend on foreign-controlled digital infrastructure, its ability to safeguard citizens' rights, ensure continuity of service, and resist external coercion may be compromised. In this regard, the discourse on "digital or technological sovereignty" intersects directly with international human rights law.

The right to privacy and data protection is recognized under Article 17 of the ICCPR[47] and Article 8 of the Charter of Fundamental Rights of the European

44. Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford: Oxford University Press, 2017).

45. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).

46. Matthias Cornelius Kettemann and Stephan Dreyer, "Benevolent Dictatorships in Cyberspace? Private Power and State Responsibility for Digital Infrastructures," *German Law Journal* 21, no. 5 (2020): 941–961.

47. United Nations, *International Covenant on Civil and Political Rights*, United Nations Treaty Series, vol. 999 (1966), 171, art. 17.

Union[48] and the right to data protection as emerging under European jurisprudence, European jurisprudence, notably Digital Rights Ireland, has reinforced the autonomous right to data protection as a cornerstone of digital sovereignty.[49]

The contemporary debate over cloud sovereignty thus encapsulates a deeper normative question: how can international law reconcile the functional globalization of data flows with the enduring principle of sovereign equality? One emerging answer lies in the development of regional digital compacts such as the EU's Data Governance Act and the proposed European Cloud Federation that seek to restore a degree of control through interoperability standards, transparency obligations, and regional infrastructure investment. However, such initiatives also risk balkanizing the global internet, as states pursue self-sufficiency through "digital borders" and "data nationalism." This delicate balance between autonomy and openness, sovereignty and cooperation, defines the legal frontier of cloud governance in the 21st century.

Ultimately, the governance of cloud infrastructures is not merely a technical challenge but a redefinition of international order. As data becomes a strategic resource akin to territory or energy, the ability to regulate, secure, and access cloud systems will increasingly determine geopolitical influence. The task of international law in this context is twofold: to articulate shared principles of accountability and due process that transcend jurisdictional fragmentation, and to ensure that the pursuit of technological sovereignty does not erode the foundational values of openness, human rights, and multilateralism that underpin the digital commons.

FINAL CONSIDERATIONS

The evolution of cloud computing has transformed the architecture of global information governance, redefining the boundaries between technological in-

48. European Union, *Charter of Fundamental Rights of the European Union*, 2012/C 326/02 (2012), art. 8.

49. Court of Justice of the European Union, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (Joined Cases C-293/12 and C-594/12), ECLI:EU:C:2014:238 (2014).

terdependence and state sovereignty. As this paper has shown, the cloud is not merely a technical infrastructure but a juridical and geopolitical space, where issues of jurisdiction, accountability, and control intersect. Its dual nature as both an enabler of innovation and a facilitator of cyber threats poses unprecedented challenges to traditional conceptions of international law and state responsibility.

The diffusion of data across jurisdictions, coupled with the dominance of a few global Cloud Service Providers (CSPs), has weakened national oversight and complicated the enforcement of privacy, security, and human rights obligations. The shared responsibility model demonstrates that technological governance is inherently distributed, yet international law has not kept pace with this diffusion of accountability. Moreover, the weaponization of cloud infrastructures by state and non-state actors underscores the urgent need for normative development in the fields of sovereignty, due diligence, and transnational cyber accountability.

To reconcile global connectivity with sovereign control, international cooperation must move beyond fragmented regulatory approaches.

For both public and private organizations, the adoption of cloud services must be accompanied by: a comprehensive risk assessment conducted at the project's design stage, in line with the principles of privacy by design and security by design; strict contractual clauses with cloud service providers, addressing data localization, subcontracting chains, and cross-border data transfers; and, a robust data governance framework jointly overseen by Data Protection Officers (DPOs) and Chief Information Security Officers (CISOs), aligned with European standards and guidance.

REFERENCES

Alvarez, Maria. "Hacktivism in the Age of Cloud Computing." *Cyber Policy Journal* 8, no. 1 (2021): 77–94.

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. "A View of Cloud Computing." *Communications of the ACM* 53, no. 4 (2010): 50–58.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

Bradshaw, Simon, Christopher Millard, and Ian Walden. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19, no. 3 (2011): 187–223.

Brousseau, Eric, and Meryem Marzouki. *Digital Sovereignty: Rethinking Sovereignty in the Digital Age*. Oxford: Oxford University Press, 2021.

Brown, Thomas. *Cybercrime and Cloud Vulnerabilities: Global Perspectives*. London: Routledge, 2021.

Butcher, John, and Irina Beridze. "What Is the State of Artificial Intelligence Governance Globally?" *The RUSI Journal* 164, nos. 5–6 (2019): 88–96.

Cartelis. "L'architecture Cloud: Les concepts clés." February 16, 2019. https://www.cartelis.com/blog/architecture-cloud/.

Catteddu, Daniele, and Giles Hogben. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. Heraklion: European Network and Information Security Agency (ENISA), 2009.

Chen, Ying. "Platform-Level Security in Cloud Services: Legal and Operational Perspectives." *International Review of Law, Computers & Technology* 33, no. 4 (2019): 345–362.

Court of Justice of the European Union. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (Joined Cases C-293/12 and C-594/12), ECLI:EU:C:2014:238. 2014.

Craig, Thomas. "Cloud Computing and the Politics of Data Sovereignty: A Global Governance Perspective." *Journal of Information Technology & Politics* 16, no. 3 (2019): 241–256.

De Filippi, Primavera, and Sean McCarthy. "Cloud Computing: Legal Issues in a Global Context." *Computer Law & Security Review* 28, no. 6 (2012): 588–596.

European Union. *Charter of Fundamental Rights of the European Union*, 2012/C 326/02. 2012.

Floridi, Luciano. *The Ethics of Artificial Intelligence and Digital Sovereignty*. Springer, 2022.

Google. *Threat Horizons H1 2024 Threat Horizons Report*. 2024. https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf.

Hernandez, Daniel. *Weaponizing the Cloud: Cyber Offense in the Digital Age*. New York: Columbia University Press, 2020.

Johnson, Laura. *Shared Responsibility in Cloud Security: Legal and Technical Considerations*. Cambridge: Cambridge University Press, 2020.

Kaspersky. *Threat Intelligence Report: Cloud-Based Exfiltration Patterns 2019–2023*. 2023.

Kettemann, Matthias Cornelius, and Stephan Dreyer. "Benevolent Dictatorships in Cyberspace? Private Power and State Responsibility for Digital Infrastructures." *German Law Journal* 21, no. 5 (2020): 941–961.

Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2015.

Kumar, Subhash, and Rajiv Singh. "IaaS, PaaS, SaaS: Risk Management in Cloud Computing." *Journal of Cybersecurity Law* 12, no. 3 (2021): 101–120.

Lee, Jason, and Robert Patterson. "APT Campaigns and the Exploitation of Commercial Cloud Platforms." *Journal of Strategic Cyber Studies* 11, no. 2 (2024): 88–112.

Li, Xin. "Cloud Exploitation and Cyber-Operations: The Rise of Virtualized Attacks." *Journal of Digital Security Studies* 9, no. 4 (2021): 212–234.

Lopez, Felipe. "SaaS and Cloud Governance: A Shared Responsibility Model." *Cyber Policy Journal* 9, no. 2 (2022): 55–78.

Marin, Edward. *European Digital Sovereignty and the Challenges of Cloud Dependence*. Oxford: Oxford University Press, 2023.

Martinez, Patricia. *Cross-Border Cloud Services and International Legal Compliance*. Oxford: Oxford University Press, 2021.

Microsoft. "Modern-Day Witchcraft: A New Breed of Hybrid Attacks by Ransomware Operators." October 3, 2024.

Müller, Hans, and Katrin Weiss. *Critical Infrastructure and Cloud Attacks: Legal and Technical Perspectives*. Springer, 2022.

Netskope. *Cloud Security Threat Report 2023*. 2023.

Nguyen, Thi. "Ransomware and Cryptocurrency Mining in Cloud Environments." *Journal of Cybersecurity Studies* 14, no. 2 (2021): 45–67.

Okafor, Chinedu. "Sovereignty and State Responsibility in Cloud-Based Cyber Operations." *International Law Review* 47, no. 1 (2022): 33–56.

Patel, Rahul. "State-Sponsored Cyber Operations and Cloud Security Challenges." *International Review of Law, Computers & Technology* 33, no. 3 (2019): 213–231.

Pohle, Julia, and Thorsten Thiel. "Digital Sovereignty: Rhetoric and Reality." *Internet Policy Review* 9, no. 4 (2020). https://policyreview.info/articles/analysis/digital-sovereignty-rhetoric-and-reality.

Rossi, Paolo. *International Law and Cybersecurity Governance*. Oxford: Oxford University Press, 2020.

Schneier, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: W. W. Norton & Company, 2018.

Sciences Po – École de la Recherche. *European Sovereignty in Artificial Intelligence: A Competence-Based Perspective*. November 8, 2024.

Sciences Po – École de la Recherche. *Souveraineté Numérique*. Paris, 2025.

Smith, John. *Cybercrime and Cloud Vulnerabilities: An Emerging Threat Landscape*. London: Routledge, 2020.

Svantesson, Dan Jerker B. *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, 2017.

Thales. "Cloud Resources Have Become Biggest Targets for Cyberattacks, Finds Thales." June 25, 2024.

TLP.CLEAR. *Cloud Computing: État de la Menace Informatique*. République française, February 19, 2025.

Torres, Alejandro. *International Legal Governance of Cloud-Enabled Cyber Operations*. Cambridge: Cambridge University Press, 2022.

United Nations. *International Covenant on Civil and Political Rights*. United Nations Treaty Series, vol. 999. 1966.

Vie Publique. "Cloud Computing : L'ANSSI Dresse un État de la Menace." February 26, 2025.

Williams, James, and Ling Zhao. "Ransomware and Data Theft in Cloud Environments." *Journal of Cybersecurity Studies* 15, no. 1 (2022): 33–57.

Received on 24/10/2025

Approved on 07/11/2025