

International law

UDK 341.231:004.738.5

DOI <https://doi.org/10.5281/zenodo.17130590>

From Territorial to Information Sovereignty: The Evolution of Statehood in International Law

Maryna Chekh,

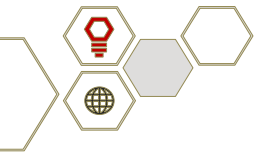
Ph.D student, Department of Philosophy

Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Accepted: 22.08.2025 | Published: 31.08.2025

Abstract: The principle of sovereignty has historically functioned as the cornerstone of international law, beginning with the Peace of Westphalia (1648) [1], which enshrined the territorial integrity and political independence of states as fundamental values. Later, these principles were codified in the UN Charter (1945), which reinforced sovereignty through the doctrines of non-intervention and jurisdictional equality. For centuries, the state's control over territory and population remained the defining characteristic of sovereignty. However, the rapid expansion of cyberspace and the emergence of the global information order have fundamentally disrupted this traditional paradigm. Digital interconnectedness erodes the classical model of territorial control, as demonstrated by transnational cyber phenomena such as the 2007 cyberattacks against Estonia and the jurisdictional controversy in *United States v. Microsoft Ireland*. In parallel, Ukrainian scholars emphasize that sovereignty today cannot be fully realized without protecting information infrastructure, cultural autonomy, and resilience to hybrid threats.

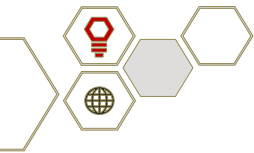
The **purpose** of this article is to examine how sovereignty has evolved from its territorial origins to encompass digital and informational dimensions, to assess the



existing doctrinal and normative gaps, and to propose a coherent conceptualization of “information sovereignty” in international law. The **methods** are historical-legal and comparative to trace the evolution of sovereignty and assess its informational dimension. Case selection was guided by three criteria: (1) **relevance** to sovereignty disputes in cyberspace and information flows (e.g., Estonia cyberattacks, Microsoft Ireland case); (2) **diversity** of models from different regions (China’s cyber sovereignty, the EU’s digital sovereignty via GDPR, Russia’s information space doctrine, and Ukraine’s hybrid warfare experience); and (3) **normative significance**, focusing on cases that shaped international legal debate (e.g., Tallinn Manual, GDPR). Analysis combined **doctrinal interpretation** of legal sources (UN Charter, Montevideo Convention, Tallinn Manual) with **comparative case analysis**, examining how states balance information security, human rights, and global governance. This dual method ensures both theoretical coherence and practical relevance.

The **results** of the study indicate that while there are existing models of sovereignty in the digital age—such as “cyber sovereignty” in China, “digital sovereignty” in the European Union, and “information space sovereignty” in Russia and Ukraine—there is still no unified doctrine of “information sovereignty” that would integrate territorial principles with the requirements of information security and transnational data governance. This doctrinal fragmentation creates significant gaps in international law, particularly concerning cross-border data flows, state responsibility for cyber operations, and the balance between sovereignty and global communication freedoms.

The **conclusions** emphasize the urgent need for multilateral dialogue and the development of an international normative framework on information sovereignty. Such a framework should reconcile state authority with the realities of digital globalization, providing mechanisms for cooperation, conflict prevention, and the protection of both security and fundamental human rights in cyberspace. The article argues that information sovereignty should not be seen as a restrictive or isolationist



principle but rather as an adaptive evolution of classical sovereignty, capable of ensuring stability, resilience, and legitimacy in the information age.

Keywords: sovereignty, information sovereignty, international law, cyber law, digital sovereignty, state jurisdiction.

**Від територіального до інформаційного суверенітету:
еволюція державності в міжнародному праві**

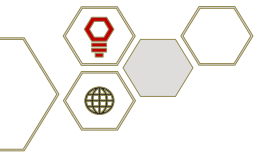
Чех Марина Олександрівна,

аспірант кафедри філософії

Національного юридичного університету імені Ярослава Мудрого,

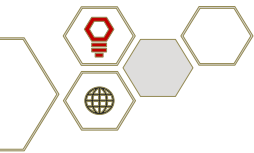
Харків, Україна

Анотація: Принцип суверенітету історично виступав наріжним каменем міжнародного права, починаючи з Вестфальського миру 1648 року [1], який закріпив територіальну цілісність та політичну незалежність держав як фундаментальні цінності. Згодом ці принципи були кодифіковані у Статуті ООН (1945), що посилив значення суверенітету через доктрину невтручання та рівності юрисдикцій. Протягом століть контроль держави над територією та населенням залишався визначальною характеристикою суверенітету. Проте стрімкий розвиток кіберпростору та становлення глобального інформаційного порядку суттєво порушили цю класичну парадигму. Цифрова взаємопов'язаність розмиває традиційну модель територіального контролю, що наочно ілюструють такі приклади, як кібератаки проти Естонії 2007 року та юрисдикційна суперечка у справі *United States v. Microsoft Ireland*. Водночас українські науковці підкреслюють, що сьогодні суверенітет неможливо забезпечити без захисту інформаційної інфраструктури, культурної автономії та стійкості до гібридних загроз.



Мета статті полягає у з'ясуванні еволюції суверенітету від його територіальних витоків до цифрового та інформаційного вимірів, аналізі наявних доктринальних та нормативних прогалин, а також у формулюванні узгодженої концепції «інформаційного суверенітету» в міжнародному праві. **Методи** мають історико-правовий та порівняльний характер і застосовуються для простеження еволюції суверенітету та оцінки його інформаційного виміру. Відбір кейсів здійснювався за трьома критеріями: (1) **релевантність** до спорів про суверенітет у кіберпросторі та сфері інформаційних потоків (наприклад, кібератаки проти Естонії, справа *Microsoft Ireland*); (2) **різноманітність моделей з різних регіонів** (кіберсуверенітет Китаю, цифровий суверенітет ЄС у межах GDPR, доктрина інформаційного простору Росії та досвід України в умовах гібридної війни); та (3) **нормативна значущість**, із фокусом на кейсах, що вплинули на розвиток міжнародно-правових дебатів (наприклад, *Tallinn Manual*, GDPR). Аналіз поєднує доктринальне тлумачення правових джерел (Статут ООН, Монтевідеоська конвенція, *Tallinn Manual*) з порівняльним аналізом кейсів, у межах якого досліджується, як держави балансують між інформаційною безпекою, правами людини та глобальним управлінням. Такий подвійний підхід забезпечує як теоретичну цілісність, так і практичну релевантність дослідження.

Результати дослідження засвідчують, що хоча існують різні моделі суверенітету в цифрову епоху — «кіберсуверенітет» у Китаї, «цифровий суверенітет» у Європейському Союзі, концепції «суверенітету в інформаційному просторі» в Росії та Україні, — все ще бракує єдиної доктрини «інформаційного суверенітету». Така доктрина могла б поєднати територіальні принципи з вимогами інформаційної безпеки та управління транскордонними потоками даних. Відсутність узгодженості створює серйозні прогалини в міжнародному праві, зокрема у сфері регулювання транскордонних даних, визначення відповідальності держав за кібероперації



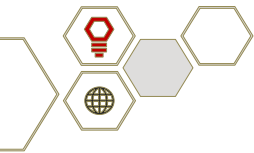
та забезпечення балансу між суверенітетом і глобальними свободами комунікації.

Висновки підкреслюють нагальну потребу у започаткуванні багатостороннього діалогу та виробленні міжнародних нормативних рамок інформаційного суверенітету. Такі рамки мають узгодити державний суверенітет із реаліями цифрової глобалізації, забезпечивши механізми співпраці, запобігання конфліктам та захисту безпеки поряд із дотриманням фундаментальних прав людини в кіберпросторі. У статті стверджується, що інформаційний суверенітет не слід розглядати як обмежувальний чи ізоляціоністський принцип, натомість він є адаптивною еволюцією класичного суверенітету, здатною забезпечити стабільність, стійкість та легітимність у добу інформаційного суспільства.

Ключові слова: суверенітет; інформаційний суверенітет; міжнародне право; кіберправо; цифровий суверенітет; юрисдикція держави

Problem Statement and Relevance. Traditionally, sovereignty has been understood as the ultimate authority of states within their territory and over their population. Since the Peace of Westphalia (1648) [1], it has served as a foundational principle of international law and relations. Yet globalization, digitalization, and cyberspace now erode traditional sovereignty. States face threats such as disinformation, cyberattacks, and extraterritorial disputes over data jurisdiction.

For Ukraine, sovereignty is existential: hybrid warfare weaponizes information flows. As Mykhailo Buromenskyi observes, “the state must protect not only its territorial borders but also its informational borders, which are increasingly decisive for national security” [8, p. 42]. In a broader context, UNESCO (2021) stressed that “the infodemic accompanying the COVID-19 crisis highlighted how disinformation threatens not only public health but also the sovereign capacity of states to safeguard democratic institutions” [9, p. 14]. This experience underscores that information sovereignty is not a purely theoretical construct but a vital dimension of resilience



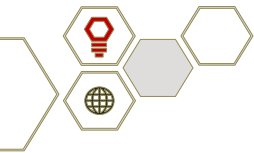
in times of crisis. The pandemic demonstrated that misinformation, if left unchecked, can destabilize political institutions as effectively as military aggression, thereby reinforcing the necessity of developing legal and normative frameworks that treat information flows as a matter of sovereignty.

Analysis of Recent Research. Classical scholarship codified sovereignty through the UN Charter (1945) [4] and the Friendly Relations Declaration (1970) [10]. Shaw and Cassese detail its foundations. Krasner described sovereignty as “organized hypocrisy,” underscoring its contested nature.

Digital scholars emphasize new challenges: DeNardis links internet governance to geopolitics; Goldsmith & Wu show states reasserting power online; Deibert analyzes China’s cyber doctrine; Chander explores GDPR’s extraterritorial effects.

Ukrainian contributions expand the debate. Horbulin links information sovereignty to survival; Danyliuk frames it as national security; Holovko-Havrysheva emphasizes balancing technology, rights, and governance; Kyrychenko stresses authenticity and security of information.

Although a considerable body of scholarship has examined the challenges posed by globalization, digitalization, and cyberspace to the classical notion of sovereignty, current debates remain fragmented. Studies of “digital sovereignty” often focus on specific regional or national approaches—such as the European Union’s emphasis on data protection, China’s policy of cyber-sovereignty, or Russia’s push for sovereign internet regulation—without providing a holistic and comparative framework. Similarly, Ukrainian and Eastern European scholarship has highlighted the security dimension of information flows in the context of hybrid warfare, but these contributions are usually treated in isolation from broader international legal discourse. What remains underdeveloped is a unified doctrine of information sovereignty that bridges traditional territorial principles with the pressing demands of information security, cultural autonomy, and transnational data governance. The absence of such a conceptual framework limits the ability of international law to respond coherently to emerging threats, from cross-border



disinformation campaigns to jurisdictional disputes over digital infrastructure and data.

Objectives of the Article. The overarching aim of this article is to conceptualize and assess “information sovereignty” as a viable and necessary category of contemporary international law. To achieve this aim, the article sets out several interrelated objectives:

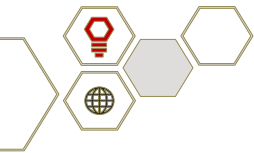
1. To trace the intellectual and legal evolution of sovereignty from its origins in the Westphalian system, through its codification in the UN Charter, to its transformation under conditions of digital globalization. This provides the necessary doctrinal foundation for understanding how informational dimensions have emerged alongside traditional territorial and political aspects.

2. To analyze and compare the principal models of sovereignty in the digital age. Particular attention will be devoted to China’s model of cyber-sovereignty, the European Union’s regulatory approach to data protection and digital governance, Russia’s strategy of internet isolation and control, and Ukraine’s experience of defending information space under conditions of hybrid warfare. This comparative approach allows for the identification of both divergences and potential areas of convergence.

3. To evaluate the feasibility of formulating “information sovereignty” as a coherent international legal principle. This entails examining whether and how existing norms of territorial integrity, non-intervention, and human rights law can be adapted to the realities of the information domain.

4. To propose conceptual and normative directions for an international legal framework that could integrate information sovereignty into global governance. This includes identifying potential mechanisms, such as multilateral treaties, confidence-building measures, and international monitoring institutions, capable of balancing state authority, human rights, and the free flow of information.

5. To outline the practical implications of information sovereignty for global security, interstate cooperation, and the resilience of democratic institutions.



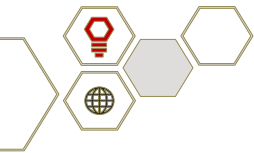
By articulating these implications, the article seeks to provide a foundation for future scholarly debate as well as for informed policymaking at both national and international levels.

Main Body. Sovereignty has long served as the cornerstone of international law and global order. Emerging from the Peace of Westphalia (1648), it crystallized the principle that states exercise supreme authority over their territory and domestic affairs without external interference. As Stephen Krasner famously notes, sovereignty is “organized hypocrisy” because while it remains a normative ideal, it has always been contested and adapted to changing historical contexts [11, p. 3]. The Montevideo Convention (1933) [18] further codified this principle, requiring states to have a defined territory, permanent population, government, and capacity for foreign relations [2, p. 159].

Yet, the advent of cyberspace and digital interconnectedness has radically challenged this traditional paradigm. Laura DeNardis argues that “internet governance is as much about geopolitics and national security as it is about technical coordination” [12, p. 5]. The borderless nature of data flows erodes the efficacy of territorial jurisdiction, raising pressing questions of who has the authority to regulate information in an interconnected world. Similarly, Jack Goldsmith and Tim Wu highlight how the internet has not escaped state control but rather “reconfigured the scope and methods of regulation” [13, p. 51].

Ukrainian scholars also emphasize that the digital domain reshapes sovereignty. Mykhailo Buromenskyi writes that “the state must now protect not only its territorial borders but also informational borders, which are increasingly decisive for national security” [8, p. 42]. Likewise, Oksana Holovko-Havrysheva underscores that sovereignty in the information age must be reconceptualized “as a balance between technological independence, human rights, and integration into global governance” [16, p. 11].

Classical Sovereignty in International Law. The concept of sovereignty occupies a central place in the history of international law, serving as the primary



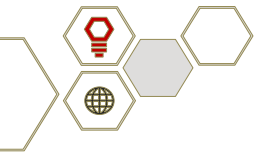
organizing principle of the international system. Since the Peace of Westphalia (1648) [1], sovereignty has been tied to territorial integrity and political independence, establishing a framework of states as legally equal entities. The durability of this principle testifies to its adaptability, yet its classical form remains foundational to understanding contemporary debates about information sovereignty.

Territorial Integrity and Political Independence. The Westphalian settlement (1648) [1] is often regarded as the symbolic origin of the modern sovereign state system. Although historians debate the extent of its revolutionary impact, the treaties established a normative order premised on the recognition of exclusive territorial authority. As Antonio Cassese explains, the core Westphalian legacy lies in “the absolute competence of each state within its territory and the prohibition of outside interference” [3, p. 49].

This principle of territorial supremacy became embedded in customary international law. As Malcolm Shaw emphasizes, sovereignty “denotes the totality of international rights and duties recognized by international law as residing in an independent territorial unit” [2, p. 488]. States enjoy the competence to regulate all matters within their boundaries—political, legal, economic, and cultural—without external intrusion.

Ukrainian scholars also stress the enduring relevance of the Westphalian conception. Oleksandr Zadorozhnii observes that “principles of Westphalian sovereignty were not only formally absorbed into the practice of international law, but also remain essential for understanding challenges to Ukraine’s territorial integrity today” [19, p. 37]. The historical resonance of sovereignty is particularly acute in Ukraine’s struggle against external aggression, where defending territorial boundaries represents a direct continuation of the Westphalian tradition.

Sovereignty and the United Nations Charter. The UN Charter (1945) [4] codified sovereignty as the organizing principle of the post–World War II international order. Article 2(1) affirms that the “Organization is based on the principle of the sovereign equality of all its Members,” echoing the Westphalian



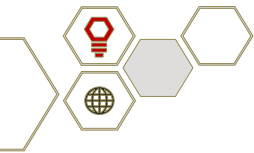
insistence on formal equality. Article 2(4) further prohibits “the threat or use of force against the territorial integrity or political independence of any state,” entrenching sovereignty as a legal bulwark against aggression.

As Cassese notes, the Charter represents both continuity and innovation: “The UN Charter crystallized in legal form the concept of sovereignty, while at the same time introducing limits through the development of collective security and human rights” [3, p. 52]. Similarly, Shaw explains that sovereignty under the UN system is not merely a right but also a responsibility, constrained by the need to maintain international peace and security [2, p. 490].

Ukrainian perspectives also underline the Charter’s importance. Volodymyr Vasylenko highlights that “the prohibition of the use of force enshrined in Article 2(4) is fundamental for the protection of Ukraine’s sovereignty and independence” [20, p. 22]. In Ukraine’s case, the Charter framework has provided the legal vocabulary through which the international community condemns violations of its sovereignty, especially following Russia’s annexation of Crimea in 2014 and full-scale aggression in 2022.

Non-Intervention Rule and Jurisdictional Sovereignty. A corollary of territorial sovereignty is the principle of non-intervention. This doctrine prohibits external actors from interfering in the internal or external affairs of a sovereign state. It was codified in the UN General Assembly’s Declaration on the Inadmissibility of Intervention (1965) [21] and reaffirmed in the Friendly Relations Declaration (1970) [10].

Cassese defines the principle succinctly: “Non-intervention is the logical extension of sovereignty. If states are to be equal and independent, they must be free from external dictates in matters essentially within their domestic jurisdiction” [3, p. 56]. Shaw likewise stresses that jurisdictional sovereignty means “the competence of a state to exercise, within its territory, the functions of a government, and to exclude any other state from exercising them” [2, p. 495].



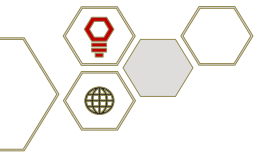
In Ukrainian legal discourse, non-intervention holds particular significance given persistent foreign interference. As Petro Rabinovych points out, “jurisdictional sovereignty presupposes the exclusive competence of Ukraine to regulate its own political, legal, and cultural processes, which cannot be subject to external dictates” [22, p. 84]. This interpretation underscores how the classical principle of sovereignty remains directly applicable to contemporary geopolitical realities.

The classical model of sovereignty—developed through the Westphalian system, codified in the UN Charter, and reinforced through the non-intervention rule—remains indispensable to international law. Its enduring appeal lies in its capacity to provide stability, equality, and predictability in relations among states. Yet, as Ukrainian and international scholars alike observe, these principles are not merely abstract legal constructs but have urgent practical significance in the defense of national independence and territorial integrity.

While globalization and digitalization are rapidly transforming the contexts in which sovereignty operates, the classical foundations continue to serve as the normative anchor. As will be discussed in subsequent sections, the challenge is to reconcile these territorial principles with the realities of cyberspace and informational interdependence, without undermining the core values of non-intervention, equality, and territorial integrity.

Digitalization and the Challenge to Traditional Sovereignty. The emergence of the digital age has introduced profound challenges to the classical, territorially anchored model of sovereignty. Global connectivity, borderless communication, and the rise of powerful non-state digital actors have weakened the capacity of states to exercise exclusive authority within their borders. While sovereignty remains a cornerstone of international law, its meaning and application are increasingly strained in the context of cyberspace.

Global Connectivity and Borderless Communication. Digitalization has radically transformed the circulation of information, creating a global public sphere that transcends national borders. Internet infrastructure allows instantaneous



communication across continents, undermining the state's ability to control flows of data. As Malcolm Shaw notes, "the principle of territorial sovereignty presupposes that a state can regulate all activities within its borders; yet the very nature of cyberspace undermines this presupposition" [2, p. 1040].

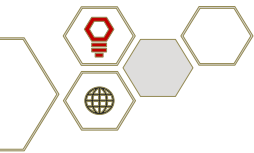
Antonio Cassese similarly underscores the challenge, observing that "modern information technologies reduce the effectiveness of territorial borders as instruments of control" [3, p. 62]. The unprecedented ease of cross-border communication means that traditional mechanisms of jurisdiction and censorship no longer guarantee exclusive control over a population's information environment.

Ukrainian scholars link this erosion of borders directly to national security. Volodymyr Vasylenko warns that "the globalization of information flows and the spread of borderless communication make states vulnerable to manipulation of public opinion and information aggression" [20, p. 41]. In Ukraine's experience, disinformation campaigns and hostile narratives spread digitally have been as destabilizing as physical incursions.

Cloud Services and Global Platforms. Another dimension of digitalization is the weakening of territorial control over data. With the rise of cloud services, social media platforms, and transnational digital corporations, states struggle to enforce jurisdiction within their borders. Data may be stored on servers located abroad, raising complex questions about which state has authority over that information.

As Jack Goldsmith and Tim Wu argue, "the architecture of the Internet undermines the assumption that data and communication flows are anchored to any one territorial space" [13, p. 137]. This reality complicates both law enforcement and sovereignty-based claims.

For Ukraine, the challenge is acute. Petro Rabinovych emphasizes that "the dependence of national information space on foreign digital platforms creates risks of external control and limits the state's ability to guarantee information security" [22, p. 112]. Reliance on platforms such as Facebook, Google, and Twitter illustrates how sovereignty in the digital domain is diffused among corporate actors that do not

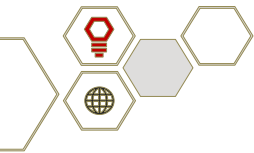


always align with state interests. As Zuboff observes, “the pandemic intensified the asymmetry of power between governments and digital corporations, as emergency measures shifted critical infrastructures into private hands” [23, p. 237]. She further notes that “by outsourcing crisis management to platforms, states weakened their own sovereignty in the digital sphere, creating dependencies that may outlast the emergency” [23, p. 240]. This finding suggests that information sovereignty cannot be secured solely through territorial or legislative means; it also requires states to reconsider the distribution of authority between public and private actors. The pandemic exposed how emergency reliance on transnational platforms may erode state capacity for independent decision-making, turning corporations into de facto arbiters of sovereignty in the digital space.

Case Law and State Practice. Estonia Cyberattacks (2007). A landmark event demonstrating the sovereignty challenge in cyberspace was the 2007 cyberattacks against Estonia, widely attributed to Russian actors. Following the relocation of a Soviet-era war memorial in Tallinn, Estonia experienced weeks of distributed denial-of-service (DDoS) attacks that paralyzed government websites, banks, and media outlets.

Michael Schmitt, analyzing the case, notes that “the Estonia incident illustrated the vulnerability of even advanced states to external cyber operations and raised unresolved questions regarding whether such operations violate sovereignty and amount to an unlawful intervention” [5, p. 9]. The Tallinn Manual, developed in response, attempted to clarify that “a cyber operation which causes physical damage or loss of functionality in another state’s territory constitutes a breach of sovereignty” (Rule 5) [5].

From Ukraine’s perspective, Estonia’s experience was a precursor to its own. As Oleksandr Zadorozhnii observes, “the Estonian cyberattacks demonstrated the inability of traditional sovereignty to ensure security in cyberspace, a lesson that became highly relevant for Ukraine after 2014” [19, p. 118].



Microsoft Ireland Case (2013–2018). Another critical sovereignty dispute concerned the *United States v. Microsoft Corp.* case, often called the “Microsoft Ireland case.” U.S. authorities sought access to emails stored on servers located in Dublin, Ireland, raising the question of whether American courts could compel a company to produce data stored outside U.S. territory.

As the Second Circuit held in 2016, the U.S. could not unilaterally apply its warrants extraterritorially: “Congress did not intend the Stored Communications Act’s warrant provisions to apply extraterritorially, and therefore they cannot compel Microsoft to produce information stored abroad” [24, p. 220].

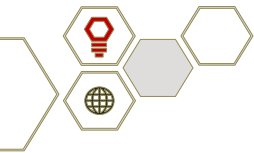
This case highlighted the limits of state sovereignty in the digital domain. As Jennifer Daskal explains, “the Microsoft case exposed the tension between traditional territorial sovereignty and the borderless nature of data flows, forcing reconsideration of jurisdictional principles” [25, p. 472].

Ukrainian experts drew similar conclusions. Vasylenko noted that “the Microsoft Ireland case showed how data stored abroad challenges the effectiveness of national jurisdiction and requires new international agreements” [20, p. 77].

The digital age has redefined the scope of sovereignty. While classical sovereignty was territorially grounded, digitalization has produced an environment where communication, data, and influence transcend borders with unprecedented ease. Estonia’s cyberattacks revealed the vulnerability of state infrastructures to external actors, while the Microsoft Ireland case underscored the difficulty of applying traditional jurisdictional concepts to extraterritorial data storage.

Both English and Ukrainian scholarship converge on the view that territorial sovereignty alone is insufficient to ensure security and independence in the information era. This recognition drives the current debates on “information sovereignty”, where states seek to reclaim authority over digital flows while preserving global connectivity

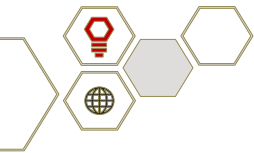
Information Sovereignty as a Legal Concept. The digital transformation of societies has created a pressing need to reconceptualize traditional legal doctrines of



sovereignty. While cyberspace was once envisioned as a realm beyond state authority, developments in regulation, geopolitics, and international law demonstrate a clear trend toward asserting state and supranational authority over information flows. This trend crystallizes in the emerging concept of *information sovereignty*. Unlike *cyber sovereignty*—which emphasizes control of network infrastructure—or *digital sovereignty*—which broadly refers to autonomy in technological and infrastructural terms—information sovereignty foregrounds the normative and legal authority of states (or regional organizations) over data and communicative processes within their jurisdiction.

Existing Definitions: Comparative Models. The Chinese approach to information sovereignty is arguably the most robust in asserting state primacy. It frames cyberspace as an extension of state territory, legitimizing extensive monitoring and filtering practices. As Deibert notes, China views information sovereignty as the “legitimate right of the state to regulate cyberspace in the same manner as its physical territory” [14, p. 33]. This conception, deeply embedded in the principle of political stability, aligns sovereignty with ideological security.

The European Union offers a different model, one oriented toward individual rights and data protection. The General Data Protection Regulation (GDPR) operationalizes the EU’s notion of digital and informational sovereignty by granting citizens control over their personal data irrespective of where processing occurs. As Chander observes, “the GDPR extends the EU’s sovereignty beyond its borders by imposing obligations on foreign entities that process European data” [15, p. 120]. Building on this trajectory, Shaw and Graham argue that “COVID-19 has become a catalyst for Europe’s renewed push for digital sovereignty, accelerating initiatives on data governance and platform regulation” [26, p. 59]. They further underline that “the pandemic revealed the strategic vulnerability of states reliant on external digital infrastructures, strengthening arguments for data localization and sovereignty-based regulation” [26, p. 63]. This development reflects a broader trend in which crises function as accelerators of sovereignty debates, pushing regional and national actors



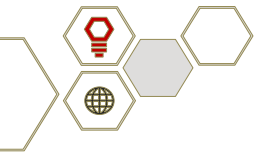
to consolidate authority over digital infrastructures. The EU's response illustrates that information sovereignty is not only defensive, aimed at countering disinformation, but also proactive, aimed at structuring global digital governance on normative grounds.

In contrast, the Russian Federation's doctrine of information security places emphasis on national security and control over domestic information space. As Kovalčuk argues, Russia frames informational sovereignty as a response to perceived threats of "foreign manipulation and disinformation campaigns," positioning information space as "a field of strategic rivalry" [27, p. 77]. This approach resembles China's, but is even more explicitly securitized.

Ukrainian scholarship, responding to the realities of Russian aggression and hybrid warfare, has emphasized information sovereignty as an existential necessity. According to Horbulin [6, p. 56], Ukraine must build a resilient system of informational sovereignty to counter "the weaponization of information flows" that undermine statehood. Similarly, Danyliuk [7, p. 211] stresses that Ukraine's sovereignty cannot be preserved without effective control over its digital information space, as disinformation campaigns are "tools of destabilization targeting state institutions and democratic processes." These insights ground the Ukrainian conception of information sovereignty in survival and national defense.

Distinction from Cyber Sovereignty and Digital Sovereignty. Conceptually, information sovereignty differs from both *cyber sovereignty* and *digital sovereignty*. Cyber sovereignty often focuses on state control of critical infrastructure and ICT networks. Digital sovereignty, especially in the EU discourse, denotes autonomy in technological development and supply chains (e.g., semiconductor independence, cloud infrastructure). By contrast, information sovereignty concerns authority over data itself: who owns it, who can regulate it, and under what legal frameworks.

As Laura DeNardis argues, "information sovereignty involves struggles over who has the legitimate authority to control information flows, infrastructures, and standards that affect global communication" [12, p. 57]. This moves beyond

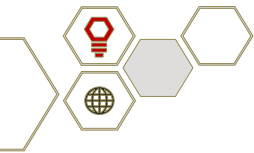


technical infrastructure to address legal norms and political values. In practice, information sovereignty entails regulating the collection, storage, dissemination, and protection of information in ways that reflect a state's legal order.

Ukrainian scholars, while acknowledging the overlaps, insist on this distinction. As Kyrychenko [17, p. 133] notes, the Ukrainian context demonstrates that *informational sovereignty* is primarily about “ensuring truth, authenticity, and security of information” rather than technological autonomy per se. In this sense, Ukrainian thought emphasizes the substantive quality of information flows rather than merely technical or infrastructural control.

Toward an International Normative Framework. The absence of an agreed international definition remains a major obstacle. Current international law only indirectly addresses aspects of information sovereignty through doctrines of jurisdiction, non-intervention, and the protection of human rights. The Tallinn Manual on the International Law Applicable to Cyber Warfare (2017) suggests that state sovereignty extends into cyberspace, prohibiting interference with cyber infrastructure [5, p. 19]. However, it does not clearly resolve the issue of informational authority.

Recent UN initiatives, such as the Global Digital Compact (2023) [28], seek to establish principles of inclusivity, trust, and accountability in digital governance, but remain non-binding. Similarly, EU strategic projects like EuroStack (2025) [29] represent efforts to operationalize digital and informational sovereignty through infrastructural independence. Yet these initiatives illustrate fragmentation: while some states seek human-rights-based frameworks, others prioritize national security and control. As Kurbalija emphasizes, “post-COVID geopolitics has placed digital governance at the center of international law, with information sovereignty emerging as a contested but unavoidable principle” [30, p. 150]. He further notes that “the pandemic accelerated the shift from viewing information flows as a technical issue to recognizing them as a core matter of sovereignty and security in international relations” [30, p. 154]. This shift demonstrates that information sovereignty has



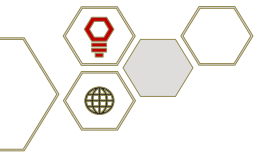
evolved from an academic notion into a pressing geopolitical reality. States that fail to engage in shaping these emerging norms risk marginalization, while proactive actors may set the standards that define the digital order of the coming decades.

Ukrainian contributions underscore the urgency of an international framework. As Vasylenko [31, p. 88] argues, without internationally agreed standards of informational sovereignty, “small and vulnerable states remain disproportionately exposed to disinformation, cyber aggression, and external manipulation.” This reflects the broader normative dilemma: how to reconcile state sovereignty with international obligations under human rights law and free expression norms (Art. 19) [32].

Ultimately, a coherent doctrine of information sovereignty must integrate principles of territorial sovereignty, jurisdiction, and human rights. It should acknowledge the right of states to protect information space while upholding the universality of rights to access and share information. As DeNardis puts it, “the future of global order will be shaped not only by physical borders but by the normative rules governing the flow of information” [33, p. 142].

Conclusions. The analysis of sovereignty’s evolution from a territorial to an informational paradigm demonstrates that while sovereignty remains a cornerstone of international law, it requires reinterpretation in light of technological transformation. The need for harmonization of rules is evident: without common standards, states resort to unilateral measures such as data localization, extraterritorial regulation, or national firewalls, which fragment cyberspace and risk undermining the global information order [12, p. 57], [31, p. 87].

A multilateral dialogue or convention on information sovereignty should therefore be advanced, building upon precedents such as the UN Charter’s reaffirmation of sovereign equality (UN Charter 1945, Art. 2) [4], the Tallinn Manual’s clarification of cyber norms [5, p. 102], and emerging initiatives like the Global Digital Compact [28, p. 3]. Ukrainian scholarship underscores that for states exposed to hybrid warfare, such as Ukraine, a binding international framework on

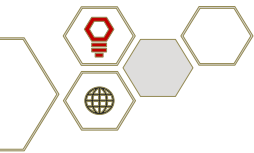


information sovereignty is not only a matter of legal coherence but of existential national security [6, p. 214], [17, p. 43].

The experience of the COVID-19 pandemic also offers valuable lessons for Ukraine in conceptualizing information sovereignty. The infodemic revealed by UNESCO (2021) showed that disinformation can paralyze democratic decision-making as effectively as armed aggression. Zuboff demonstrated how dependence on private digital infrastructures weakens sovereign capacities in times of crisis, while Shaw and Graham highlighted how the EU transformed pandemic vulnerabilities into an impetus for regulatory consolidation. As Kurbalija notes, the pandemic has repositioned information sovereignty as a central category of international law and global governance. For Ukraine, these insights underline the urgency of integrating pandemic-era experiences into legislative and strategic reforms. Embedding information sovereignty into national security law, ensuring transparency and accountability in cooperation with global platforms, and aligning with EU digital sovereignty initiatives would not only address vulnerabilities exposed during the pandemic but also strengthen Ukraine's position in shaping emerging international norms.

To operationalize these insights, specific measures could be proposed for Ukrainian legislation:

1. Introduce a dedicated legal framework defining the principles, rights, and responsibilities associated with information sovereignty, including state obligations for protecting critical digital infrastructure and personal data.
2. Establish an independent national body tasked with monitoring compliance with information sovereignty norms, coordinating with both domestic agencies and international partners.
3. Incorporate information sovereignty explicitly into national defense and cybersecurity legislation, addressing hybrid threats, disinformation campaigns, and the protection of strategic digital assets.



4. Mandate transparency, data-sharing protocols, and cooperative frameworks with global digital platforms to prevent foreign manipulation while safeguarding freedom of expression.

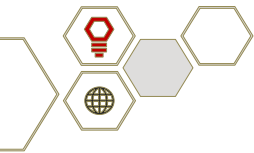
5. Harmonize Ukrainian regulations with EU digital sovereignty strategies and emerging international agreements to ensure interoperability, legal consistency, and support for multilateral governance.

At the same time, significant questions for future research remain unresolved. How should international law balance state sovereignty with the transnational information flows that underpin the global economy [15, p. 738]? Can the right to information and freedom of expression be reconciled with state claims to control and security [14, p. 121]? Should information sovereignty be conceived primarily as a defensive doctrine against disinformation and hybrid threats [7, p. 96], or as a proactive principle ensuring digital rights and freedoms in cyberspace [34, p. 12]? Moreover, how can enforcement mechanisms be designed to ensure compliance without further fragmenting the digital space?

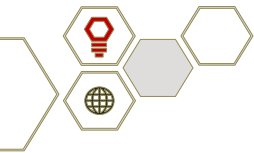
Addressing these challenges requires not only legal innovation but also a philosophical commitment to reconciling sovereignty with universal human rights. Ukraine's ongoing struggle illustrates the urgency of this task, as the defense of territorial integrity is inseparable from the protection of the informational domain [31, p. 89]. A working definition of information sovereignty that is both legally sound, normatively balanced, and operationally implementable may thus become one of the most significant contributions to international law in the digital era.

Bibliography

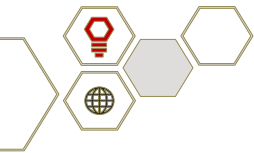
1. Peace of Westphalia: Peace Treaty between the Holy Roman Emperor and the King of France and their respective Allies. 1648. Yale Law School, Lillian Goldman Law Library. URL: https://avalon.law.yale.edu/17th_century/westphal.asp?utm_source=chatgpt.com (date of access: 06.06.2025).



2. Shaw M. *International law*. 8th ed. Cambridge: Cambridge University Press, 2017.
3. Cassese A. *International law*. 2nd ed. Oxford: Oxford University Press, 2005.
4. *Charter of the United Nations*. 26 June 1945, 1 UNTS XVI. URL: <https://www.un.org/en/about-us/un-charter> (date of access: 06.06.2025).
5. Schmitt M. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press, 2017.
6. Горбулін, В. *Гібридна війна: вижити і перемогти* [Hybrid War: Survive and Win]. Київ: НІСД, 2017.
7. Данилюк, О. В. *Інформаційна безпека України: сучасні виклики та загрози* [Information Security of Ukraine: Contemporary Challenges and Threats]. Київ: Либідь, 2020.
8. Буроменський, М. *Право і суверенітет у цифрову епоху* [Law and Sovereignty in the Digital Age]. Київ: Юрінком Інтер, 2018.
9. UNESCO. *The COVID-19 pandemic and the infodemic: A human rights approach to information sovereignty*. Paris: UNESCO, 2021. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000377438> (date of access: 06.06.2025).
10. UNGA Resolution 2625 (XXV). *Declaration on principles of international law concerning friendly relations and cooperation among states*. 24 October 1970.
11. Krasner S. *Sovereignty: Organized hypocrisy*. Princeton: Princeton University Press, 1999.
12. DeNardis L. *The global war for Internet governance*. New Haven: Yale University Press, 2014.
13. Goldsmith J., Wu T. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press, 2006.
14. Deibert R. *Black code: Surveillance, privacy, and the dark side of the Internet*. Toronto: Signal, 2015.



15. Chander A. The coming global battle over data. *UC Davis Law Review*. 2019. Vol. 52, no. 2. P. 711–760. DOI: <https://doi.org/10.2139/ssrn.3311885>
16. Головка-Гавришева, О. Цифровий суверенітет: між правами людини та державними інтересами [*Digital Sovereignty: Between Human Rights and State Interests*]. *Вісник Львівського університету. Серія юридична*. 2020. Вип. 71. С. 112–124. URL: <http://law.lnu.edu.ua/journals/visnyk71> (date of access: 06.06.2025).
17. Кириченко, А. *Інформаційний суверенітет України: виклики та перспективи* [*Information Sovereignty of Ukraine: Challenges and Prospects*]. Харків: Право, 2021.
18. *Montevideo Convention on the rights and duties of states*. 26 December 1933. 165 LNTS 19.
19. Задорожній, О. *Міжнародне право в сучасному світі* [*International Law in the Contemporary World*]. Київ: Юридична думка, 2014.
20. Василенко, В. *Суверенітет і міжнародне право: український вимір* [*Sovereignty and International Law: The Ukrainian Dimension*]. Київ: Наукова думка, 2015.
21. UNGA Resolution 2131 (XX). *Declaration on the inadmissibility of intervention*. 21 December 1965.
22. Рабінович, П. *Основи загальної теорії права та держави* [*Foundations of the General Theory of Law and State*]. Львів: Світ, 2016.
23. Zuboff S. The age of surveillance capitalism in pandemic times. *Journal of Information Technology & Politics*. 2020. Vol. 17, no. 3. P. 233–245. DOI: <https://doi.org/10.1080/19331681.2020.1789446>
24. *United States v. Microsoft Corp.* 829 F.3d 197 (2d Cir. 2016).
25. Daskal J. Borders and bits. *Vanderbilt Law Review*. 2018. Vol. 71, no. 2. P. 465–523. DOI: <https://doi.org/10.2139/ssrn.3094282>



26. Shaw T., Graham M. Pandemics, platforms, and power: COVID-19 and the future of digital sovereignty. *Global Policy*. 2022. Vol. 13, suppl. 1. P. 55–68. DOI: <https://doi.org/10.1111/1758-5899.13103>
27. Kovalčuk I. Russia's information sovereignty doctrine: Between security and control. *Journal of Strategic Studies*. 2020. Vol. 43, no. 1. P. 75–96. DOI: <https://doi.org/10.1080/01402390.2019.1701970>
28. United Nations. *Global digital compact: Zero draft*. New York: United Nations, 2023. URL: <https://www.un.org/techenvoy/global-digital-compact>
29. European Commission. *EuroStack: Strategic roadmap for European cloud and data sovereignty*. Brussels: European Commission, 2025. URL: <https://ec.europa.eu/digital-strategy> (date of access: 06.06.2025).
30. Kurbalija J. Post-COVID digital geopolitics and information sovereignty. *Journal of Cyber Policy*. 2023. Vol. 8, no. 2. P. 142–160. DOI: <https://doi.org/10.1080/23738871.2023.2201479>
31. Василенко, М. Інформаційний суверенітет у міжнародному праві [Information Sovereignty in International Law]. *Український журнал міжнародного права*. 2022. № 2. С. 83–92.
32. *International Covenant on Civil and Political Rights (ICCPR)*. United Nations, 1966. URL: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (date of access: 06.06.2025).
33. DeNardis L. *The Internet in everything: Freedom and security in a world with no off switch*. New Haven: Yale University Press, 2020.
34. European Commission. *State of the digital decade 2025: Keep building the EU's sovereignty and digital future (Annex I)*. Brussels: European Commission, 2025. URL: <https://ec.europa.eu/digital-strategy> (date of access: 06.06.2025).