UDC 341.231:004.738:004.056
DOI https://doi.org/10.51989/NUL.2025.4.39

DEFINING INFORMATION SOVEREIGNTY: WHAT IS INFORMATION SOVEREIGNTY?

Chekh Maryna Oleksandrivna,
Postgraduate Student at the Department of Philosophy
Yaroslav Mudryi National Law University

This article explores the reconceptualization of sovereignty in the digital era through the emerging paradigm of information sovereignty. Whereas traditional international law associated sovereignty with territory and borders, digitalization has elevated information and data flows to a domain of sovereign authority. The article argues that information sovereignty must be understood as a multidimensional practice involving autonomy, authority, and responsibility: the ability to act independently in cyberspace, the legal competence to regulate information flows, and the normative obligation to balance national interests with human rights and global interdependence.

The analysis unfolds in four parts. First, it develops a working definition of information sovereignty by drawing on doctrinal debates in international law, European and Chinese legal frameworks, and Ukrainian scholarly contributions shaped by the realities of hybrid warfare. Second, it examines comparative models of sovereignty in the digital age: China's cyber sovereignty emphasizing defensive control, the European Union's rights-based data sovereignty exemplified by the GDPR, and the United States' market-driven approach. Third, it reflects on normative tensions, particularly the conflict between national security imperatives and universal human rights, and the challenge of reconciling state sovereignty with cyberspace as a global commons. Finally, it proposes a typology of information sovereignty – defensive, economic, and regulatory – that provides analytical clarity to the competing interpretations of sovereignty in the digital domain.

The article concludes that information sovereignty should not be understood as a return to absolute territorial control but as a layered practice of governance. For Ukraine, this involves simultaneously defending against disinformation, building domestic digital capacities, and aligning with European regulatory standards. More broadly, the typology highlights that information sovereignty is less a fixed status than an ongoing negotiation between security, economy, and law. Recognizing this dynamic character is essential for designing governance frameworks that preserve both state autonomy and the openness of the global digital order.

Key words: *information sovereignty, digital sovereignty, cyber sovereignty, data sovereignty, international law, human rights, Ukraine, GDPR, cyber security, global commons.*

Чех Марина. Визначення інформаційного суверенітету: що таке інформаційний суверенітет?

У статті досліджується переосмислення суверенітету в цифрову епоху крізь призму формування нового парадигмального підходу – інформаційного суверенітету. Якщо традиційне міжнародне право пов'язувало суверенітет із територією та кордонами, то цифровізація висунула інформаційні та дані потоки як нову сферу суверенного авторитету. Доводиться, що інформаційний суверенітет слід розуміти як багатовимірну практику, що поєднує автономію, владні повноваження та відповідальність: здатність діяти незалежно у кіберпросторі, юридичну компетенцію регулювати інформаційні потоки та нормативний обов'язок балансувати між національними інтересами, правами людини та глобальною взаємозалежністю.

Аналіз розгортається у чотирьох напрямах. По-перше, розробляється робоче визначення інформаційного суверенітету на основі доктринальних дебатів у міжнародному праві, європейських та китайських правових підходів, а також українських досліджень, сформованих у реаліях гібридної війни. По-друге, здійснюється порівняння моделей суверенітету в цифрову добу: китайська концепція «кіберсуверенітету», що акцентує на оборонному контролі; право-орієнтована парадигма «суверенітету даних» у ЄС, уособлена Регламентом GDPR; а також ринково-орієнтований підхід США. По-третє, висвітлюються нормативні суперечності, зокрема конфлікт між імперативами національної безпеки та універсальними правами людини, а також проблема узгодження державного суверенітету з кіберпростором як глобальним спільним надбанням. Нарешті, пропонується типологія інформаційного суверенітету – оборонного, економічного та регулятивного, яка надає аналітичну чіткість конкуруючим інтерпретаціям суверенітету у цифровій сфері.

Стаття доходить висновку, що інформаційний суверенітет не слід тлумачити як повернення до абсолютного територіального контролю, а як багаторівневу практику врядування. Для України це означає одночасно протидію дезінформації, розвиток власних цифрових спроможностей і гармонізацію з європейськими регулятивними стандартами. У ширшій перспективі типологія демонструє, що інформаційний суверенітет – це не фіксований статус, а постійний процес переговорів між безпекою, економікою та правом. Усвідомлення цієї динаміки є ключем до формування механізмів врядування, які збережуть як автономію держав, так і відкритість глобального цифрового порядку.

Ключові слова: *інформаційний суверенітет, цифровий суверенітет, кіберсуверенітет, суверенітет даних, міжнародне право, права людини, Україна, GDPR, кібербезпека, глобальні спільні надбання.*

The accelerating digitalization of global society has fundamentally altered the meaning of sovereignty in international law and politics. Once defined primarily in terms of territorial control, population, and exclusive jurisdiction, sovereignty is now challenged by the transnational and intangible nature of information flows. Information, data infrastructures, and algorithmic systems have become strategic resources that transcend borders, creating new arenas of power, vulnerability, and regulation. This transformation calls for a rethinking of sovereignty not as a static principle inherited from the Westphalian system, but as a dynamic practice adapted to the digital era.

The emergence of "information sovereignty" captures this shift. It reflects the growing recognition that control over information is as vital to national security, economic autonomy, and political legitimacy as control over territory. From China's doctrine of cyber sovereignty to the European Union's rights-based paradigm of data governance, states and regional organizations are reinterpreting their sovereign prerogatives in light of digital infrastructures and global information ecosystems. Yet, the diversity of models also reveals deep normative tensions: between security and human rights, autonomy and interdependence, national interest and the global commons.

Ukraine's experience illustrates the urgency of this debate. Exposed to hybrid warfare, disinformation campaigns, and cyberattacks, Ukraine demonstrates that information sovereignty is not an abstract concept but a condition of state survival. At the same time, Ukraine's alignment with European legal frameworks signals that sovereignty in the digital domain is also a matter of normative choice and geopolitical orientation.

This article reframes sovereignty in the digital sphere through conceptual, comparative, and normative lenses. It proceeds in four steps. First, it unpacks the concept of information sovereignty by distinguishing autonomy, authority, and responsibility. Second, it compares the leading models of digital sovereignty across China, the EU, and transatlantic contexts. Third, it reflects on the normative tensions between national interests, human rights, and the global commons. Finally, it maps a typology of information sovereignty – defensive, economic, and regulatory – proposing an analytical framework for understanding contemporary transformations of sovereignty in the digital age.

Unpacking the Concept: Toward a Working Definition of Information Sovereignty. The emergence of "information sovereignty" as a concept reflects the deep transformation of international law in the digital era. Traditionally, sovereignty was tied to territory, borders, and state jurisdiction. Today, however, information – transnational, intangible, and constantly circulating—has itself become a domain of sovereign authority. This shift requires a reconceptualization of statehood, responsibility, and governance in cyberspace.

1. Clarifying the notion of information as a domain of sovereign authority. The notion that information constitutes a sovereign domain is relatively new in international legal discourse. According to S. Liulko, information sovereignty should be understood as "the capacity of the state to establish and ensure legal, political, and institutional control over information flows within its jurisdiction" [1, p. 15]. This formulation mirrors classical definitions of sovereignty but relocates its material basis: from land and population to data, digital infrastructures, and informational exchanges.

French doctrinal debates emphasize the geopolitical stakes of this reconceptualization. The French Senate, in its report on digital sovereignty, stresses that "sovereignty is no longer limited to borders and territory: it extends to the control of infrastructures, technologies, and above all data" [2, p. 4]. This represents a profound reorientation of the sovereign function, where information –rather than territory – becomes the primary vector of power.

Yet, as Ruohonen provocatively observes, this move risks paradox. Information sovereignty is often presented as a Westphalian translation into cyberspace: the "capacity to govern" in digital space. But this, he warns, may be a treachery of images, reproducing old logics onto a fundamentally new domain [3, p. 223]. Information is not territorial, and its regulation requires novel models of distributed authority.

Ukrainian scholars have sharpened this idea under the conditions of hybrid war. S. Kutsepal underscores that information sovereignty is "inseparable from national security, since the integrity of informational borders can be as decisive as territorial ones" [4, p. 37]. Here, sovereignty over information is not an abstract principle but a survival condition for the state in the context of cyberwarfare and foreign disinformation campaigns.

This confirms that information sovereignty can be framed as both a defensive shield and a positive capacity for governance. It designates the state's right to regulate information flows, its obligation to protect its informational environment, and its strategic capacity to leverage information for development.

2. Distinguishing autonomy, authority, and responsibility in digital governance. To build an operational definition of information sovereignty, it is necessary to disaggregate its dimensions into autonomy, authority, and responsibility.

First, autonomy refers to the state's ability to act independently in cyberspace. The European Parliament notes that autonomy in digital governance implies reducing dependence on foreign technologies and infrastructures, especially in cloud computing and critical data storage [5, p. 12]. This is the essence of strategic independence: the ability to maintain informational integrity without external coercion.

Second, authority refers to the legal and institutional competence to establish rules. In the European Union, the General Data Protection Regulation (GDPR) provides a paradigmatic example of authority exercised beyond borders: "data belonging to European citizens are subject to European law, regardless of the place of processing" [6, Art. 3]. This extraterritorial application illustrates sovereignty reconfigured as regulatory power. Similarly, the Chinese model of cyber sovereignty, codified in the Cybersecurity Law (2017), claims authority over all digital activities within national networks [7, p. 9].

Third, responsibility arises from the fact that digital sovereignty is not exercised in isolation but affects global flows. As the Internet Society stresses, sovereignty over information cannot mean "absolute control" without undermining the openness of the internet; instead, it entails responsibility for balancing national interests with the global commons [8, p. 18].

Thus, responsibility has a double meaning: internally, the state must protect citizens' rights, especially privacy and freedom of expression; externally, it must avoid fragmenting cyberspace through unilateral restrictions. Amnesty International highlights how China's use of cyber sovereignty as a tool of repression illustrates the dangers of neglecting this responsibility: "invoking sovereignty to justify censorship and surveillance fundamentally contradicts human rights obligations" [9, p. 3].

The distinction between autonomy, authority, and responsibility allows us to see information sovereignty not as a monolithic claim but as a layered concept. It is simultaneously about independence from foreign control, the legal right to regulate, and the normative duty to respect rights and international obligations.

Information sovereignty is the capacity of the state, within international law, to autonomously regulate, protect, and responsibly govern information and data flows under its jurisdiction, balancing national interests, individual rights, and global interdependence.

This definition integrates the conceptual insights of French legal doctrine, the normative practices of the EU and China, and the urgent realities of Ukraine. It positions information sovereignty not merely as an extension of territorial control but as a multidimensional practice of authority, autonomy, and responsibility in the digital sphere.

Comparative Perspectives on Sovereignty in the Digital Age. The reconfiguration of sovereignty in the digital era represents one of the most challenging questions in contemporary international law and political theory. Information and communication technologies (ICTs), global data infrastructures, and algorithmic governance mechanisms increasingly bypass traditional borders. Yet, states continue to insist on their sovereign prerogatives, adapting them to cyberspace. The comparative study of national and regional approaches reveals at least three major models: the Chinese conception of cyber sovereignty, the European paradigm of data sovereignty and the General Data Protection Regulation (GDPR), and the transatlantic tensions between the United States and the European Union.

1. The Chinese Model of Cyber Sovereignty. The People's Republic of China has become the leading advocate of a sovereignty-based conception of cyberspace. The official discourse describes cyberspace as an extension of national territory where states enjoy "absolute rights of control, security, and governance" [10, p. 44]. This perspective departs from the early U.S. vision of the internet as a borderless "global commons".

The Cybersecurity Law of the PRC (2017) codified this principle, stipulating that all networks within Chinese jurisdiction are subject to national regulation, including data storage and censorship obligations [7, p. 9]. Later, the Data Security Law (2021) reinforced the requirement of data localization, making the export of "important data" subject to state review [11, p. 15].

Scholars interpret this as a threefold strategy: (1) ensuring political control over information, (2) guaranteeing technological security through domestic innovation, and (3) structuring data governance for strategic advantage [12, p. 92]. Yik Chan Chin and Ke Li argue that China promotes a "defensive sovereignty", oriented toward insulating its informational environment from external interference, while simultaneously exporting its model abroad through infrastructure projects and standards [13, p. 118].

However, human rights organizations warn that this model equates sovereignty with authoritarian control. Amnesty International describes China's cyber sovereignty as "a tool of repression, enabling pervasive censorship and mass surveillance" [9, p. 3]. The paradox, as Ruohonen notes, is that China "invokes sovereignty to justify practices that undermine the universality of rights and the openness of the internet" [3, p. 225].

Ukrainian authors underline the geopolitical risks of such a model. Dubov, analyzing cyberspace as a new dimension of conflict, stresses that the Chinese strategy of control provides resilience against hybrid threats but simultaneously erodes the idea of cyberspace as a shared commons [14, p. 141]. In this sense, China's cyber sovereignty can be understood as both a shield against external vulnerabilities and an instrument of internal domination.

2. European Data Sovereignty and the GDPR Paradigm. In contrast, the European Union has developed a rights-based model of digital sovereignty, which combines individual data protection with extraterritorial regulation. The General Data Protection Regulation (GDPR), adopted in 2016, defines personal data as subject to European law whenever they concern EU citizens, regardless of the location of processing [6, Art. 3]. This embodies what Bradford has called the "Brussels Effect" – the capacity of the EU to impose its standards globally through market power [15, p. 7].

The GDPR institutionalizes the idea of data sovereignty as the right of individuals and states to control the conditions of data collection, processing, and transfer. The French Commission nationale de l'informatique et des libertés (CNIL) emphasizes that sovereignty means "ensuring that European citizens' data are governed by European values and laws, and not by foreign jurisdictions" [16, p. 12].

This framework was strongly influenced by the Snowden revelations of 2013, which exposed the extraterritorial reach of U.S. surveillance through the Patriot Act. As the Innovation News Network reports, "the debate on data sovereignty accelerated when Europeans realized their personal data stored in foreign clouds could be accessed by U.S. intelligence" [17, p. 5].

European initiatives such as GAIA-X, a federated cloud infrastructure project, further reflect the ambition to achieve technological autonomy. The French Senate insists that sovereignty in the digital sphere must not only protect fundamental rights but also preserve strategic independence in infrastructure and innovation [2, p. 6].

Nevertheless, this model is not free from tension. Critics argue that excessive data localization could undermine the openness of digital markets and slow down innovation [18, p. 22]. Moreover, as Hummel et al. note, there remains a semantic ambiguity between "digital sovereignty" (a broad political project), "data sovereignty" (focused on personal data), and "information sovereignty" (emphasizing control over flows) [12, p. 9].

Yet, the European model remains unique in its integration of sovereignty with human rights. As the Conseil économique, social et environnemental (CESE) argues, "European sovereignty in the digital age cannot be conceived as purely national; it must be collective, normative, and oriented toward the protection of rights" [19, p. 14].

3. Digital Sovereignty in Transatlantic Contexts (EU and US). The transatlantic dialogue illustrates profound divergences in digital governance. While the EU promotes an integrated regulatory framework, the United States relies on a fragmented, market-driven approach. Yi Shen notes that whereas China applies cyber sovereignty defensively, "the United States extends its digital influence globally through corporate power and extraterritorial surveillance" [10, p. 48].

The absence of a comprehensive federal data protection law in the U.S. leaves regulation to sector-specific norms (e.g., HIPAA for health, COPPA for children) or state initiatives, most prominently California's Consumer Privacy Act (CCPA). The European Council on Foreign Relations (ECFR) stresses that "this fragmentation contrasts with the EU's single, rights-based framework, creating recurrent conflicts over transatlantic data transfers" [15, p. 10].

Indeed, the Schrems I (2015) and Schrems II (2020) decisions of the Court of Justice of the EU invalidated U.S.–EU data transfer agreements (Safe Harbor and Privacy Shield), precisely because American surveillance laws failed to guarantee an adequate level of protection. As Ruohonen highlights, this conflict reveals the paradox of sovereignty: "the EU insists on protecting its citizens' informational integrity, but in doing so it asserts jurisdiction beyond its borders, challenging the U.S. model of open markets" [3, p. 227].

Recent European Parliament resolutions emphasize the need for "digital solidarity" among democratic allies, calling on the U.S. to converge toward European standards [5, p. 13]. However, as Hnatiuk observes, U.S. strategies still prioritize technological leadership and innovation dominance, while the EU focuses on regulatory power and normative diffusion [20, p. 55].

The Internet Society reminds us that both models, despite their differences, shape the global governance of cyberspace: "the clash between sovereignty-based regulation

and market-based openness is not merely transatlantic but defines the future of the digital commons" [8, p. 18].

The comparative analysis demonstrates that sovereignty in the digital age is not a uniform concept but a contested field of legal and political experimentation. China reinterprets sovereignty as defensive control, prioritizing state security and political authority. The European Union frames sovereignty as rights-based regulation, balancing autonomy with the universality of human rights. The United States embodies a model of market-driven extension, relying on corporate power and extraterritorial practices rather than formal regulation.

These divergences illustrate the paradox identified by Ruohonen: "digital sovereignty is simultaneously about the assertion of national authority and the erosion of global openness" [3, p. 229]. For Ukraine and other states facing hybrid threats, as Kutsepal underlines, the stakes are existential: sovereignty over information becomes a condition of national survival [21, p. 38].

In sum, the debate on information and digital sovereignty is not only about governance models but also about the very redefinition of sovereignty in a borderless, yet increasingly contested, digital order.

Normative Tensions and Dimensions. The problem of information sovereignty cannot be reduced to questions of technical control or administrative regulation. At its core, it is a normative issue, reflecting the tensions between state interests, individual rights, and the global commons. The digital sphere, unlike physical territory, is transnational by design. This generates profound challenges for the traditional Westphalian conception of sovereignty, which presumes clear borders and exclusive jurisdiction [22, p. 11]. In the digital era, sovereignty is increasingly negotiated at the interface of security imperatives, normative frameworks for human rights, and the collective responsibility to preserve cyberspace as a common good.

1. Information sovereignty and the pursuit of national interests. States often conceptualize information sovereignty as an extension of their national security doctrines. 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" [23, p. 42]. This security-driven perspective frames information sovereignty primarily as a defensive tool against disinformation, cyberattacks, or foreign surveillance. For instance, the Russian Federation has explicitly linked its doctrine of "sovereign internet" to the need for "information security" and "resilience against external influence" [24].

However, national interest goes beyond security. Information sovereignty is also tied to economic competitiveness, technological autonomy, and the ability to shape global regulatory standards. The European Union's emphasis on "strategic autonomy" in digital policy reflects precisely this broader understanding [25]. By promoting data localization and building its own digital infrastructure, the EU attempts to reconcile sovereignty with participation in the global economy. This tension between openness and control illustrates the complexity of national interests in the digital domain.

2. Human rights considerations in digital regulation. While states assert sovereignty to defend national interests, information governance must also be reconciled with the protection of human rights. The UN Human Rights Council has consistently affirmed that "the same rights that people have offline must also be protected online" [26]. Yet, in practice, sovereignty claims often conflict with the universality of rights. The Chinese model of cyber sovereignty, for example, prioritizes state control over freedom of expression, resulting in censorship and mass surveillance [27, p. 7].

In contrast, the European Union frames data sovereignty through the language of fundamental rights. The General Data Protection Regulation (GDPR) explicitly grounds its provisions in the right to privacy and data protection enshrined in the Charter of Fundamental Rights of the EU [6]. This demonstrates that sovereignty in the information space can be exercised not only as a tool of control but also as a framework for rights protection. As DeNardis stresses, governance of information flows is "a human rights issue as much as a geopolitical one" [28, p. 58].

The challenge lies in balancing sovereignty with rights. Excessive data localization, justified in the name of sovereignty, may restrict global access to information and impede innovation. Conversely, unregulated information flows risk undermining the right to privacy, as shown by recurring transatlantic disputes over data transfers [29]. Sovereignty, in this sense, becomes a double-edged sword: it can serve as a shield for rights or as a pretext for restricting them.

3. Reconciling sovereignty with the global commons. Finally, the question arises whether information and cyberspace can be conceptualized as part of the global commons. Some scholars argue that treating information as a purely sovereign resource risks fragmenting the digital sphere into "digital sovereignties" and undermining its collective potential [30, p. 94]. The analogy with environmental governance is telling: just as climate change cannot be addressed within national borders alone, so too the regulation of cyberspace requires multilateral approaches.

This perspective is evident in initiatives such as the UN's "Global Digital Compact," which aspires to establish shared principles for information governance [31]. Yet, reconciling national sovereignty with global governance remains difficult. As the European Court of Human Rights has noted, states retain "a margin of appreciation" in regulating information flows, but must do so in ways consistent with international obligations [32, p. 12].

In practice, reconciling sovereignty and the global commons may require a layered approach: sovereignty as responsibility, rather than sovereignty as absolute authority. This reframing aligns with the concept of "sovereignty as stewardship," where states maintain primary jurisdiction but remain accountable to international norms and cooperative frameworks [33, p. 65]. By adopting such a model, sovereignty can be reinterpreted not as the antithesis of global governance, but as its building block.

The normative dimensions of information sovereignty illustrate the profound complexity of digital governance. Sovereignty is simultaneously a vehicle of national interest, a tool for protecting rights, and a challenge to the global commons. Its interpretation varies across jurisdictions and normative traditions, but its essence lies in balancing competing imperatives. To secure the legitimacy of sovereignty in the information age, states must move beyond a narrow focus on control and embrace a responsibility-based model that harmonizes security, rights, and global cooperation.

Mapping a Typology of Information Sovereignty. The emergence of "information sovereignty" has opened a conceptual space that transcends traditional notions of territorial sovereignty while responding to the geopolitical, economic, and normative pressures of the digital age. As scholars emphasize, this concept remains contested, encompassing terms such as digital sovereignty, cyber sovereignty, and data sovereignty, each reflecting different emphases and political projects (Couture & Toupin, 2019, p. 95; Hummel et al., 2021, p. 13). For analytical clarity, this reflection maps a threefold typology of information sovereignty: (1) defensive sovereignty, emphasizing security and resilience; (2) economic sovereignty, construing data as a strategic resource; and (3) regulatory sovereignty, focusing on law, platforms, and extraterritorial norms. This typology enables both a comparative perspective and an evaluation of normative dilemmas.

1. Defensive Sovereignty: Security and Resilience. Defensive information sovereignty highlights the state's responsibility to secure its informational domain against external aggression, disinformation, and technological dependency. In many respects, this dimension mirrors the Westphalian tradition, where sovereignty was first and foremost about defending borders [3, p. 312]. Yet, in the digital sphere, borders are porous, contested, and constantly reshaped.

The Chinese doctrine of "cyber sovereignty" represents the most forceful articulation of defensive sovereignty. China's Cybersecurity Law (2017) and Data Security Law (2021) enshrine strict localization of data and central control of information flows, justifying them as necessary for "national security" and protection against "foreign interference" [7; 11]. As Yi Shen notes, "China views cyber sovereignty primarily as defensive, an assertion of informational borders against

U.S. dominance of digital infrastructures" [10, p. 14]. This perspective was reinforced in recent analyses of Chinese AI governance, which identify three pillars of sovereignty: control of information, data regulation, and technological security [34, p. 87].

Critics, however, highlight the risks of authoritarian overreach. Amnesty International argues that China's invocation of cyber sovereignty has become "a tool of repression, restricting access to information and curtailing human rights in the name of security" [35]. This tension demonstrates the paradox of defensive sovereignty: while it protects against disinformation, it may also erode freedom of expression and individual autonomy.

The Ukrainian case illustrates a democratic variant of defensive sovereignty. Since 2014, Ukraine has confronted hybrid aggression, where disinformation campaigns, cyberattacks, and digital propaganda accompany military operations. As Kutsepal observes, "the preservation of information sovereignty is existential for Ukraine, as the erosion of informational resilience translates directly into threats to territorial integrity" [4, p. 78]. Blocking Russian propaganda outlets, enhancing cybersecurity capacity, and embedding information security into the National Security Strategy of Ukraine (2020) exemplify this defensive posture. Scholars like Dubov argue that cyberspace has become a new dimension of geopolitical confrontation, where resilience is now a "strategic imperative for sovereignty" [14, p. 144].

The French Senate report on digital sovereignty similarly stresses security as a foundation for national autonomy, noting that "resilience of digital infrastructures is a matter of sovereignty, without which no economic or normative independence is possible" [2, p. 12]. Thus, defensive sovereignty constitutes both the oldest and most urgent aspect of information sovereignty, grounding the typology in security imperatives.

1. Economic Sovereignty: Data as a Strategic Resource. Economic sovereignty emphasizes the ownership, control, and strategic use of data as a key resource of the 21st century. The Snowden revelations, which exposed the global reach of U.S. intelligence, catalyzed global debates on data sovereignty by showing that control over data flows was directly tied to economic power and political autonomy.

The European Union's GDPR (2016/679) epitomizes this perspective. Beyond protecting privacy, the regulation enshrines principles of data residency, consent, and extraterritorial applicability, thereby asserting Europe's capacity to govern data generated by its citizens regardless of where companies are located [6, Art. 3]. This "Brussels Effect" (ECFR, 2022) illustrates how regulatory power can be transformed into economic sovereignty by setting de facto global standards [36]. Commentaries from the French CNIL emphasize that "data must remain subject to the laws of the state of origin rather than those of third countries" [16]. The French Ministry of Economy further links economic sovereignty to cloud computing independence, advocating European solutions like GAIA-X to reduce dependency on U.S. providers [37].

As the Conseil économique, social et environnemental (CESE) stresses, data constitutes not only an economic asset but also a public good, whose governance implicates national interest and collective rights. This approach connects sovereignty to industrial strategy and technological competitiveness.

For Ukraine, economic information sovereignty remains an emerging concern. Analysts point to the risks of dependency on foreign cloud providers and platforms, arguing that "the economic dimension of sovereignty requires not only protection from disinformation but also the development of domestic digital industries and secure data storage capacities" [1, p. 8]. The war has underscored this vulnerability, as reliance on international platforms (such as the U.S.-based cloud storage) has proven both vital for resilience and a limitation on true economic autonomy.

Thus, economic sovereignty reframes data as a form of national wealth and strategic resource, positioning states not only as guardians but also as competitors in the global data economy [17].

3. Regulatory Sovereignty: Law, Platforms, and Extraterritorial Norms. Regulatory sovereignty concerns the legal

and normative frameworks through which states and supranational actors assert authority over digital platforms, algorithms, and cross-border information flows. While defensive and economic sovereignty emphasize protection and ownership, regulatory sovereignty is about shaping rules and extending them beyond national borders.

The EU again provides the paradigmatic case. Through instruments like the GDPR, the Digital Services Act (2022), and recent resolutions on technological sovereignty [5], the EU has cultivated what SWP calls a "multi-level approach": internal regulation combined with the external diffusion of norms. This strategy is grounded in rights-based values, making regulatory sovereignty simultaneously legal and ethical.

France's Senate report underlines that sovereignty "is not isolation but the ability to choose and impose rules, including at the international level" [2, p. 23]. This resonates with Ruohonen's interpretation of sovereignty as political capacity to govern rather than mere independence [3, p. 316].

China presents a contrasting model of regulatory sovereignty, using law as a mechanism of control rather than rights protection. The Cybersecurity Law (2016) and Data Security Law (2021) empower the state to regulate private companies, enforce data localization, and sanction cross-border transfers deemed risky to sovereignty. As Yik Chan Chin and Ke Li observe, "Chinese regulatory sovereignty prioritizes national security over individual rights, exporting a governance model where compliance is ensured through state surveillance and corporate alignment" [13, p. 211].

The United States, by contrast, lacks a comprehensive federal framework, relying instead on sectoral laws (HIPAA, CCPA) and private self-regulation. This fragmentation undermines the coherence of U.S. regulatory sovereignty but also reflects its liberal tradition of limiting state authority over markets.

Ukraine again finds itself navigating between models. By aligning with GDPR principles in its legislation, Ukraine asserts its aspiration to European regulatory sovereignty. At the same time, national security imperatives push toward stricter controls reminiscent of the Chinese model. As Hnatyuk argues, "Ukraine must develop a balanced model of digital sovereignty, combining solidarity with European allies and resilience against hybrid threats" [20, p. 92].

Mapping information sovereignty through the lenses of defensive, economic, and regulatory sovereignty provides a comprehensive framework for understanding both theoretical distinctions and practical dilemmas. Defensive sovereignty secures the informational domain, economic sovereignty transforms data into a strategic resource, and regulatory sovereignty frames the normative environment of digital governance. Together, they constitute a layered approach that highlights sovereignty's transformation in the digital age: from borders to infrastructures, from territory to data, and from autonomy to interdependence.

Ukraine's trajectory illustrates how these dimensions intertwine: defending against disinformation (defensive), building resilient digital industries (economic), and aligning with European legal frameworks (regulatory). The broader global context shows competing models – authoritarian, liberal, and rights-based – each embedding different balances of security, economy, and norms. Ultimately, information sovereignty is less a fixed state than a dynamic negotiation, where the typology outlined here provides analytical clarity for navigating its tensions and futures.

The digital revolution has unsettled the very foundations of sovereignty. No longer confined to territory and borders, sovereignty now extends to information, infrastructures, and transnational digital ecosystems. The concept of information sovereignty, though still contested, provides a vital lens for understanding this transformation. By unpacking its dimensions, comparing different national models, and mapping its typologies, this article has demonstrated that information sovereignty is both a theoretical construct and a practical necessity in the digital age.

The comparative analysis revealed divergent paths. China articulates sovereignty defensively, framing cyberspace as an extension of territorial authority to be secured against external interference. The European Union emphasizes rights-

based regulation, positioning sovereignty as a vehicle for protecting fundamental rights while also asserting extraterritorial authority through instruments like the GDPR. The United States reflects a market-driven approach, relying on corporate dominance and fragmented legal frameworks. These models are not only legal and political projects but also competing visions of digital order.

Normative tensions complicate this landscape. Information sovereignty is invoked to defend national interests, but it can also threaten human rights if reduced to control and censorship. Conversely, rights-based regulation demonstrates that sovereignty can align with universal principles, though it risks clashing with economic globalization and technological innovation. Reconciling sovereignty with the global commons remains an open challenge, requiring states to exercise authority as responsibility rather than absolute power.

Ukraine's trajectory underscores both the urgency and complexity of information sovereignty. Facing hybrid warfare and persistent disinformation, Ukraine has treated information sovereignty as a condition of survival. Yet its choice to harmonize with European legal frameworks highlights that sovereignty is not only about defense but also about normative orientation and geopolitical belonging. This dual imperative – security and integration – illustrates how information sovereignty is shaped by context, values, and strategic choice.

Ultimately, the typology of defensive, economic, and regulatory sovereignty provides a framework for navigating these dilemmas. Defensive sovereignty secures informational borders, economic sovereignty frames data as a strategic resource, and regulatory sovereignty establishes rules that extend beyond borders. Together, they show that sovereignty in the digital sphere is layered, interdependent, and dynamic.

In conclusion, information sovereignty should not be conceived as a nostalgic return to rigid territorial control. Rather, it represents the evolution of sovereignty into a multidimensional practice of governance in which autonomy, authority, and responsibility must be carefully balanced. The future of digital order will depend on whether states can reconcile national security, human rights, and global cooperation within this framework. For Ukraine and other states on the frontlines of hybrid conflict, this balance is not only a theoretical concern but an existential challenge.

BIBLIOGRAPHY:

1. Люлько С. Інформаційний суверенітет держави. Logos Science, 2019. 178–181.
2. Sénat. The duty of digital sovereignty. Paris : Sénat, 2019. P. 4.
3. Ruohonen J. The treachery of images in the digital sovereignty debate. *Digital Policy, Regulation and Governance*. 2020. Vol. 22. No. 3. P. 223–240.
4. Куцепал С. Інформаційний суверенітет та інформаційна безпека України: Виклики та реалії війни. *Poltava Law Review*. 2023. No. 1. P. 78–88.
5. European Parliament. Resolutions on technological and digital sovereignty. Brussels, 2025. P. 12.
6. GDPR. Regulation (EU) 2016/679. Brussels : Official Journal of the European Union, 2016.
7. Cybersecurity Law of the PRC. Beijing : National People's Congress, 2017.
8. Internet Society. Digital sovereignty: analysis report. Geneva, 2019.
9. Amnesty International. China: "cyber-sovereignty" as a tool of repression. Brussels, 2017.
10. Yi Shen. Cyber Sovereignty and the Governance of Global Cyberspace. *Springer*, 2016: 81–93.
11. Data Security Law of the PRC. Beijing : National People's Congress, 2021.
12. Hummel P., Couture S., Toupin S. Digital sovereignty debates: concepts and critiques. SpringerLink, 2021.
13. Chin Y.C., Li K. Sovereignty in the Cyberspace: Contestation of Concepts and Policies. *AoIR: The 22nd Annual Conference of the Association of Internet Researchers,* 2021.
14. Дубов Д. *Кіберпростір як новий вимір геополітичного суперництва*. Київ : НІСД, 2014.

15. ECFR. Europe’s digital sovereignty: from rulemaker to superpower. Brussels, 2020.
16. CNIL. The GDPR and the protection of personal data. Paris, 2018. P. 25.
17. Innovation News Network. Data sovereignty: implications and challenges. London, 2020.
18. SWP. European digital sovereignty: internal and external dimensions. Berlin, 2021.
19. CESE. For a European policy of digital sovereignty. Paris, 2020. P. 20.
20. Hnatyuk S. Geopolitical digital vision of the US and EU: digital solidarity, digital sovereignty and new cyberspace strategy. Kyiv : NISD, 2021.
21. Kutsepal S.V. Information sovereignty and information security of Ukraine. *Pravo Ukrainy*. 2021. P. 37–45.
22. Krasner S. Sovereignty: organized hypocrisy. Princeton : Princeton University Press, 1999. P. 256.
23. Buromenskyi M. International law and state information security. Kyiv : NaUKMA, 2018. P. 215.
24. SWP. Russia’s sovereign Internet law: tightening the control of online information. Berlin : Stiftung Wissenschaft und Politik, 2021.
25. CESE. Europe and digital sovereignty: exploratory opinion. Brussels : Comité économique et social européen, 2022.
26. UN General Assembly. The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/20/8, 2013.
27. Creemers R. Cyber China: upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*. 2015. Vol. 24. No. 93. P. 85–100.
28. DeNardis L. The Internet in everything: freedom and security in a world with no off switch. New Haven : Yale University Press, 2020.
29. ECFR. Europe’s digital sovereignty: from rulemaker to superpower in the age of US-China rivalry. European Council on Foreign Relations, 2021.
30. Floridi L. The fourth revolution: how the infosphere is reshaping human reality. Oxford : Oxford University Press, 2014.
31. UN. Global digital compact. United Nations, Our Common Agenda Report, 2022.
32. ECHR. Big Brother Watch and others v. the United Kingdom, Judgment. Strasbourg : European Court of Human Rights, 2018.
33. Held D. Global covenant: the social democratic alternative to the Washington Consensus. Cambridge : Polity Press, 2004.
34. Springer. Governance of AI and cyber sovereignty in China. Berlin : Springer, 2024. Amnesty International. *Digital security and repression*. 2019.
35. European Council on Foreign Relations. The geopolitics of technology: how the EU can become a global player, 2022. French Strategy for Cloud Computing & Data Sharing. 2023, March 15.

Стаття надійшла у редакцію: 29.08.2025
Стаття прийнята: 15.09.2025
Опубліковано: 27.10.2025