УДК 34:004.89
DOI https://doi.org/10.32782/chern.v4.2025.38

O. A. Shamov
Intelligent Systems Researcher,
Head of Human Rights Educational Guild
orcid.org/0009-0009-5001-0526

DIGITAL SOVEREIGNTY AND JURISDICTION OVER CROSS-BORDER AI SERVICES: FROM «CLOUD» TO «ALGORITHMIC» SOVEREIGNTY

The rapid proliferation of cross-border AI services challenges state sovereignty. The focus is shifting from infrastructure control («cloud sovereignty») to control over decision-making algorithms. This necessitates rethinking legal approaches, which are ineffective for regulating extraterritorial intelligent systems, and developing a new framework for asserting state control. Purpose. To research the evolution of the digital sovereignty concept, analyze the jurisdictional challenges of cross-border AI services, and develop a two-tiered model of «algorithmic sovereignty» to balance national interests, innovation, and international law. Methods. The research is based on dialectical, formal-legal, and comparative-legal methods. The methods of analysis, synthesis, and modeling were used to develop the author's model of algorithmic sovereignty. Results. The concept of «cloud sovereignty» is proven to be insufficient. The notion of «algorithmic sovereignty» is proposed as the state's ability to extend jurisdiction over the decision-making processes of impactful algorithms. An innovative two-tiered model is developed: the first tier for critical AI systems (mandatory audit and certification), and the second for general AI services (the principle of «jurisdiction by effect» with intermediary responsibility). Conclusion. The proposed model allows for an effective response to challenges by shifting the regulatory focus from the physical location of data to the functional impact of algorithms. This creates a mechanism to protect critical interests without digital protectionism. Future research prospects lie in developing standards for algorithm audits and harmonizing certification requirements.

Key words: digital sovereignty, algorithmic sovereignty, artificial intelligence, jurisdiction, cross-border services, BU AI Act, extraterritoriality, algorithm audit.

Шамов О. А. **ЦИФРОВИЙ СУВЕРЕНІТЕТ ТА ЮРИСДИКЦІЯ НАД ТРАНСКОРДОННИМИ ШІ-СЕРВІСАМИ: ВІД «ХМАРНОГО» ДО «АЛГОРИТМІЧНОГО» СУВЕРЕНІТЕТУ**

Стрімке поширення транскордонних ШІ-сервісів створює виклики для державного суверенітету. Дискусії зміщуються від контролю над інфраструктурою («хмарний суверенітет») до контролю над алгоритмами, що приймають рішення. Це вимагає переосмислення правових підходів, які є неефективними для регулювання екстериторіальних інтелектуальних систем, та розробки нової рамки для утвердження державного контролю. Мета. Дослідження еволюції концепції цифрового суверенітету, аналіз юрисдикційних викликів транскордонних ШІ-сервісів та розробка дворівневої моделі «алгоритмічного суверенітету» для збалансування національних інтересів та інновацій в рамках міжнародного права. Методи. Дослідження базується на діалектичному, формально-юридичному та порівняльно-правовому методах. Для розробки авторської моделі алгоритмічного суверенітету використано методи аналізу, синтезу та моделювання. Результати. Доведено, що концепція «хмарного суверенітету» є недостатньою. Запропоновано поняття «алгоритмічного суверенітету» як здатності держави поширювати юрисдикцію на процеси прийняття рішень алгоритмами, що мають значний вплив. Розроблено інноваційну дворівневу модель: перший рівень для ШІ-систем критичного значення (обов'язковий аудит та сертифікація), другий – для загальних ШІ-сервісів (принцип «юрисдикції за наслідками» з відповідальністю посередників). Висновок. Запропонована модель дозволяє ефективно реагувати на виклики, переміщуючи фокус регулювання з фізичного розташування даних на функціональний вплив алгоритмів. Це створює механізм захисту критичних інтересів без цифрового протекціонізму. Перспективи досліджень полягають у розробці стандартів аудиту алгоритмів та гармонізації вимог до їх сертифікації.

Ключові слова: цифровий суверенітет, алгоритмічний суверенітет, штучний інтелект, юрисдикція, транскордонні сервіси, Регламент ЄС про ШІ, екстериторіальність, аудит алгоритмів.

Problem Statement. The modern world order is increasingly defined not only by geopolitical and economic factors but also by technological dominance. The proliferation of artificial intelligence (AI), especially in the form of cross-border digital services provided by global tech corporations, poses a fundamental challenge to the Westphalian model of state sovereignty, which is based on the principle of territoriality. When an algorithm developed in one country, trained on data from around the world, and hosted on cloud servers in a third country makes decisions that have direct legal, economic, and social consequences for the citizens of a fourth country, the classic mechanisms of jurisdiction fail.

The problem is that traditional concepts of digital sovereignty, which emerged in response to the challenges of the global Internet, are becoming obsolete. The first wave of the struggle for digital sovereignty focused on data sovereignty – the right of a state to demand that the personal data of its citizens be stored and processed within its physical borders. This

approach, vividly embodied in data localization requirements, has proven insufficient, as the mere storage of data does not guarantee control over its use.

The second wave, which can be described as «cloud sovereignty,» shifted the emphasis to control over computational infrastructure. States began to strive for the creation of national cloud platforms or to require global providers (such as Amazon Web Services, Microsoft Azure, Google Cloud) to locate infrastructure on their territory. However, this approach also has significant limitations. The physical location of a server does not provide real control over the software code and algorithmic logic executed on it. A foreign provider may comply with infrastructure localization requirements but simultaneously use algorithms that are opaque, biased, or contrary to the public order and fundamental values of the host state.

Thus, a gap emerges between the territorially limited jurisdiction of the state and the global, decentralized nature of modern AI services. This gap creates legal «gray zones» and undermines the state's ability to perform its key functions: protecting citizens' rights, ensuring economic stability, and guaranteeing national security. An urgent practical task is to develop a new legal doctrine and toolkit that will allow state sovereignty to be extended not only to data and infrastructure but also to the very logic of artificial intelligence decision-making.

Analysis of Recent Studies and Publications. The problem of digital sovereignty and its connection to new technologies is a subject of active scientific debate. The very concept of digital sovereignty has been articulated by scholars like Pohle and Thiel (2020) as the ability of a state to exercise control over its digital infrastructure, data, and the legal frameworks governing the digital space. One of the key works explaining the mechanisms for extending this sovereignty beyond national borders is the concept of the «Brussels Effect», proposed by Anu Bradford (2020). She argues that the European Union, due to the size of its market, is capable of de facto setting global standards in areas such as data protection (GDPR) and, potentially, AI regulation through the AI Act. This market-power-based approach is one attempt to solve the jurisdictional problem. At the same time, critics note that such an approach can lead to «regulatory imperialism» and does not take into account the interests of developing countries. This regulatory outreach is underpinned by a distinct philosophical commitment; as Floridi (2021) notes, the EU's approach to AI is fundamentally human-centric, aiming to create a framework that ensures technology serves societal values and fundamental rights.

She argues that the European Union, due to the size of its market, is capable of de facto setting global standards in areas such as data protection (GDPR) and, potentially. AI regulation through the AI Act. This market-power-based approach is one attempt to solve the jurisdictional problem. At the same time, critics note that such an approach can lead to «regulatory imperialism» and does not take into account the interests of developing countries (Almada & Radu, 2024).

Researchers studying the extraterritorial application of law in the digital sphere often analyze the experience of the GDPR. For example, Dove and Chen (2021) analyze the legal grounds for the extraterritorial application of the GDPR, pointing to its far-reaching consequences for companies worldwide. However, he also emphasizes the difficulties of enforcement against entities that do not have a physical presence in the EU, which is also relevant for the future regulation of AI.

The concept of «algorithmic governance» has become central to understanding how technology platforms exercise power. Kettemann (2020) notes that private actors, particularly «Big Tech», establish rules through their algorithms that regulate communication, commerce, and access to information, challenging the state's traditional monopoly on lawmaking. This idea underscores that the struggle for sovereignty is shifting from physical space to the space of code.

Attempts to regulate cross-border Al services face fundamental jurisdictional obstacles. The traditional model of jurisdiction based on the principle of territoriality proves ineffective. The EU's attempt to solve this problem through the extraterritorial application of the AI Act (similar to the GDPR) is ambitious, but faces significant enforcement difficulties. As detailed by legal scholars like Kop (2021), the European approach aims to regulate AI systems placed on the Union market or whose output is used in the Union, regardless of the provider's location. However, if a foreign provider of a high-risk AI service has no legal presence in the EU, forcing it to comply with the Regulation's requirements, such as conformity assessment or registration in a database, will be extremely difficult. Some researchers propose the term «algorithmic sovereignty,» although its meaning is not yet settled. For instance, Srinath (2025), in the context of India, views it as the country's ability to control the development and deployment of AI to achieve strategic goals, but his analysis focuses more on industrial policy than on jurisdictional mechanisms.

At the same time, existing research leaves a key problem unresolved: how exactly can a state practically exercise its jurisdiction over complex, opaque, and cross-border algorithmic systems without resorting to extreme forms of digital protectionism, which harms innovation and global trade? While some authors, such as Covenant (2025), expertly map the «legal grey zones» and jurisdictional conflicts arising from cross-border AI, most works either state the problem or analyze existing extraterritorial models (like the «Brussels Effect»). However, they do not offer a specific, differentiated legal framework for asserting sovereignty precisely at the algorithm level. This article aims to fill this gap by developing a new model that distinguishes approaches to AI regulation based on its level of criticality for society and the state.

Formulation of the Article's Objective. The objective of this article is to develop and substantiate a two-tiered conceptual model for the implementation of algorithmic sovereignty, which will allow states to effectively extend their jurisdiction over cross-border AI services. To achieve this, the article will first analyze the evolution of the digital sovereignty concept, demonstrating the limitations of approaches based on data and «cloud» sovereignty in the context of modern AI. It will then formulate a precise definition of «algorithmic sovereignty» as a key element of state control and proceed to identify and systematize the main jurisdictional problems arising from attempts to regulate cross-border AI services. Building on this analysis, the core of the article will propose and elaborate on a two-tiered model for asserting jurisdiction. This model includes a mechanism for mandatory auditing and certification for AI systems of critical importance, alongside a model of «jurisdiction by effect» combined with intermediary responsibility for general AI services. Finally, the article will substantiate the scientific novelty of this proposed approach, arguing that it provides a necessary balance between protecting national interests, supporting innovation, and preventing the excessive fragmentation of the global digital space.

Main Results. As noted, initial attempts to assert digital sovereignty were aimed at the tangible elements of the digital economy: data as a resource and servers as physical infrastructure. This logic is understandable and directly follows from the classic understanding of sovereignty as control over territory and resources. However, the value and impact of modern technology services are determined not so much by raw data or their processing location as by an intangible element – the algorithm.

An algorithm, especially in the context of self-learning systems, is not just a set of instructions but a dynamic decision-making model. It encapsulates certain values, assumptions, and goals embedded by its developers. When such an algorithm is used for credit scoring. job candidate selection, content moderation, or even managing critical infrastructure, it exercises powers that previously belonged to state or clearly regulated private institutions.

Thus, algorithmic sovereignty can be defined as the ability of a state to establish, apply, and enforce legal, ethical, and technical standards for algorithmic systems that have a significant impact on its jurisdiction, regardless of the location of their development, training, or physical deployment. This is a transition from controlling «where» (server location) to controlling «how» (the logic of the algorithm) and «what» (the results and consequences of its decisions).

This transition is inevitable given the architecture of modern AI services. A global technology company can formally comply with data localization requirements by storing data on servers in a specific country, but at the same time use a single global AI model for their analysis, which is updated centrally in its home jurisdiction. In such a case, the state where the data is located has no control over how this data is interpreted and what decisions are made based on it. Control over infrastructure without control over logic becomes an illusion of sovereignty.

Attempts to regulate cross-border AI services face fundamental jurisdictional obstacles. The traditional model of jurisdiction based on the principle of territoriality proves ineffective. The EU's attempt to solve this problem through the extraterritorial application of the AI Act (similar to the GDPR) is ambitious but faces significant enforcement difficulties. If a foreign provider of a high-risk AI service has no legal presence in the EU, forcing it to comply with the Regulation's requirements, such as conformity assessment or registration in a database, will be extremely difficult.

On the other hand, the aggressive extraterritorial application of one's own legislation can lead to conflicts of jurisdiction. Imagine a situation: an AI system for content moderation, developed in the US where the First Amendment, protecting freedom of speech, dominates), is used in Germany (where strict laws against hate speech are in effect) and in China (where strict censorship requirements apply). Whose norms should the algorithm follow? This creates legal uncertainty for developers and can lead to the «fragmentation» of the Internet,

where companies are forced to create separate versions of their services for each major market.

The US approach, which can be described as decentralized and market-oriented, also has its flaws (Romana & Santiago, 2024). It relies on industry standards and voluntary risk management frameworks (e.g., the NIST AI Risk Management Framework). This approach fosters innovation but does not give the state sufficient leverage to protect public interests in critical areas and can lead to regulatory arbitrage, where companies choose jurisdictions with the least burdensome rules.

Scientific Novelty – a Two-Tiered Model for Asserting Algorithmic Sovereignty. To overcome these challenges, a new two-tiered model for implementing algorithmic sovereignty is proposed, which differentiates regulatory requirements depending on the level of risk and strategic importance of the AI system.

Tier 1: Mandatory Algorithmic Auditing and Certification (MAAC) for AI Systems of Critical Importance:

This tier applies to a limited list of AI systems that are recognized by the

state as critical for its functioning, security, and public order. Such systems may include:

- AI used in the management of critical infrastructure (energy, transport, water supply).
- Autonomous weapon systems and AI in military command and control.
- AI systems used in the justice and law enforcement sectors (predictive policing, facial recognition in public places).
- Algorithms that determine access to key public services and social benefits.
- AI used to manage major financial markets.

For these systems, it is proposed to introduce a regime where any provider, regardless of its jurisdiction, is obliged to undergo a mandatory audit and certification process before deploying the service on the state's territory. This process should be carried out by an authorized national body (or a supranational body, as in the case of the EU) or an accredited third party.

Unlike a simple conformity assessment declared by the developer (as provided for many high-risk systems in the AI Act), an audit under the MAAC model involves a deep technical and legal analysis. It may include:

Code and model architecture audit: checking for vulnerabilities, hidden functions, and compliance with declared characteristics.

Training data audit: analysis of datasets for bias, representativeness, and the legality of their origin.

Stress testing and robustness testing: checking the system's behavior in non-standard situations and its resilience to adversarial attacks.

Legal and ethical review: assessing the algorithm's logic for compliance with fundamental rights, the principles of the rule of law, and key societal values.

Only after successfully passing the audit and obtaining a certificate can the AI system be approved for use in the respective critical area. This approach shifts the point of control from the moment of harm (ex-post) to the market access stage (ex-ante) and gives the state real, rather than declarative, control over the most important algorithms. This is a direct implementation of algorithmic sovereignty.

Tier 2: Jurisdiction by Effect and Intermediary Responsibility:

For the vast majority of other AI services (social networks, recommendation systems, online commerce, chatbots, etc.), the MAAC regime would be overly burdensome and would stifle innovation. For this category, it is proposed to use an adapted «effects doctrine», which is well-known in antitrust and private international law.

According to this doctrine, a state can extend its jurisdiction to actions committed abroad if they have substantial and foreseeable effects on its territory. In the context of AI, this means that if a foreign AI service is systematically used by a country's citizens and has a significant impact on its market or information space, it falls under the scope of national legislation (e.g., regarding consumer protection, advertising, countering disinformation).

The key problem here is enforcement. To solve it, it is proposed to place responsibility for compliance with local norms not only on the foreign developer but also on a key accessible intermediary within the jurisdiction. Such an intermediary could be:

- A local subsidiary or official representative of the technology corporation.
- Large cloud service providers whose infrastructure hosts the service.
- Mobile application stores (Apple App Store, Google Play) that distribute the relevant application.
- Major internet service providers.

These intermediaries, having a physical and legal presence in the country, become the point of application for the law. A regulator can require them, for example, to block access to a service that violates legislation or to ensure that the service provider complies with transparency requirements or provides users with effective mechanisms for appealing AI decisions. This approach creates a powerful incentive for global companies to cooperate with national regulators and adapt their services to local requirements,

as refusal could lead to loss of market access through the actions of intermediaries.

Conclusions. This article has analyzed the evolution of the concept of digital sovereignty, which demonstrated the inadequacy of existing approaches focused on data and infrastructure control for regulating modern cross-border AI services. A transition to a new paradigm – algorithmic sovereignty – was proposed and substantiated, defined as the ability of a state to extend its jurisdiction to the decision-making logic of algorithmic systems that have a significant impact on its territory, citizens, and economy.

The main result of the research is the development of an innovative two-tiered model for asserting jurisdiction, which constitutes the scientific novelty of this work. This model offers a differentiated approach that avoids the extremes of digital isolationism and an unregulated market:

1. For AI systems of critical importance, a mechanism of mandatory audit and certification (MAAC) is proposed. This ex-ante control instrument provides the state with real leverage over the most sensitive and important algorithms, ensuring their compliance with national standards of security, law, and ethics.

2. For general AI services, a model combining «jurisdiction by effect» with the principle of key intermediary responsibility is proposed. This approach allows for the effective application of national legislation to foreign providers through locally accessible actors (subsidiaries, cloud providers, app stores), creating an effective enforcement mechanism without the need to pursue foreign companies in their home jurisdictions The proposed model meets the article's objective by creating a flexible and realistic legal framework for addressing the jurisdictional challenges associated with the cross-border nature of AI. It allows states to protect their key interests without hindering technological innovation or violating the principles of global digital cooperation.

Prospects for further research. First, the development of detailed technical standards and methodologies for conducting audits of AI systems within the MAAC model is necessary. This task requires interdisciplinary collaboration between engineers, lawyers, and ethicists. Second, it is worth exploring the possibility of concluding bilateral and multilateral international agreements on the mutual recognition of AI certification results to avoid excessive bureaucracy and create a harmonized global market for trusted AI. Third, the legal status and scope of liability of digital intermediaries in the context of AI regulation require further analysis.

References

1. Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World Oxford University Press. https://doi.org/10.1093/050/9780190088583.001.0001

2. Almada, M., & Radu, A. (2024). The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal*, 1–18. https://doi.org/10.1017/glj.2023.108

3. Kettemann, M. C. (2020). The Normative Order of the Internet. *Oxford University Press.* https://doi.org/10.1093/oso/9780198865995.001.0001

4. Srinath, V. (2025). AI Algorithmic Sovereignty in India – Dhirubhai Ambani University School of Law. *Dhirubhai Ambani University School of Law.* https://sol.daiict.ac.in/thought-leadership/ai-algorithmic-sovereignty-in-india/

5. Romana, F., & Santiago, F. (2024). A Comparative Analysis of Artificial Intelligence Regulatory Law in Asia, Europe, and America. *SHS Web of Conferences*, *204*, 07006–07006. https://doi.org/10.1051/shsconf/202420407006

6. Dove, E & Chen, J. (2021). What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e). *International Data Privacy Law*, Volume 11, Issue 2, April 2021, Pages 107–124. https://doi.org/10.1093/idpl/ipab005

7. Covenant, L. (2025). Cross-Border AI Systems and Jurisdictional Conflicts: Navigating Legal Grey Zones in Accountability. *ResearchGate.* https://www.researchgate.net/publication/391952421_Cross-Border_AI_Systems_and_Jurisdictional_Conflicts_Navigating_Legal_Grey_Zones_in_Accountability

8. Floridi, L. (2021).The European Legislation on AI: a Brief Analysis of its Philosophical Approach. *Philos. Technol.* 34, 215–222 . https://doi.org/10.1007/s13347-021-00460-9

9. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review,* 9(4). https://doi.org/10.14763/2020.4.1532

10. Kop, M. (2021). EU Artificial Intelligence Act: The European Approach to AI. *Stanford – Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue No. 2/2021.* https://law.stanford.edu/wp-content/uploads/2021/09/2021-09-28-EU-Artificial-Intelligence-Act-The-European-Approach-to-AI.pdf

Дата першого надходження рукопису до видання: 18.09.2025
Дата прийнятого до друку рукопису після рецензування: 14.10.2025
Дата публікації: 26.11.2025