


Міністерство освіти і науки України
Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ
Кафедра цивільно-правових дисциплін
Модуль Жана Моне «Цифрова трансформація прав: досвід ЄС»
DiTraRi_EU 101127785

Цифрова трансформація прав: ЄС та Україна

МАТЕРІАЛИ
ІІ-ї міжнародної науково-практичної конференції

25 квітня 2025 року

м. Харків


Міністерство освіти і науки України
Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ
Кафедра цивільно-правових дисциплін
Модуль Жана Моне «Цифрова трансформація прав: досвід ЄС»
DiTraRi_EU 101127785

Цифрова трансформація прав: ЄС та Україна

МАТЕРІАЛИ
ІІ-ї міжнародної науково-практичної конференції

25 квітня 2025 року

м. Харків

Редакційна колегія:

Олексій ЗАЙЦЕВ, кандидат юридичних наук, професор
Святослав СЛІПЧЕНКО, доктор юридичних наук, професор
Олександр ШИШКА, кандидат юридичних наук, професор
Оксана БОРТНІК, кандидатка юридичних наук, доцентка
Олена ПІХУРЕЦЬ, кандидатка юридичних наук, доцентка
Наталія ШИШКА, кандидатка юридичних наук, доцентка
Світлана ЯСЕЧКО, кандидатка юридичних наук, доцентка
Олена ЧЕРНЕНКО, кандидатка юридичних наук

Адреса редакційної колегії:
61080, Україна, м. Харків, пр. Льва Ландау, 27,
Харківський національний університет внутрішніх справ,
ННИ № 1, кафедра цивільного, трудового та господарського права,
тел.: (057) 73-98-154, (057) 73-98-049
e-mail: ditrari.eu@gmail.com

Ц85 ***Цифрова трансформація прав: ЄС та Україна :*** матеріали ІІ-ї міжнародної науково-практичної конференції (25 квітня 2025 року, м. Харків) / За ред. С. О. Сліпченка, О. Л. Зайцева, О. Р. Шишки. Харків : ХНУВС, 2025. 170 с.

До матеріалів увійшли тези наукових доповідей науковців, практичних діячів, викладачів та здобувачів вищої освіти, що присвячені викликами та засадами цифрової трансформації в ЄС та в Україні; здійсненню прав людини у цифровому просторі ЄС та України; безпечному та справедливому цифрового простору ЄС та України; цифровим правам в приватному праві ЄС та України; цифровому публічному простору в ЄС та в Україні; цифровізації правосуддя ЄС та України; правовому регулюванню використання алгоритмів та систем штучного інтелекту в ЄС та в Україні.

У матеріалах збережено стиль, орфографію, пунктуацію авторських текстів. Відповідальність за зміст наукових доповідей несуть автори.

.

УДК 342.7:342.951:341.171(4-6ЄС+477)

© ХНУВС, 2025

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1784 (Last accessed: 21.04.2025).

Науковий керівник: ***Володимир ДРИШЛЮК*****,** кандидат юридичних наук, доцент, завідувач кафедри державно-правових дисциплін інституту права та безпеки Одеського державного університету внутрішніх справ.

ON THE ISSUE OF THE DIGITAL SOVEREIGNTY OF THE EU

Chernenko Olena,
PhD in Law,
Associate Professor of the Department of Public Administration and Law,
National University "Yuri Kondratyuk Poltava Polytechnic"

Cherviatsova Alina,
PhD in Law, Associate Professor,
Senior Researcher of Human Rights Centre,
University of Ghent, Brussels, Belgium,
Coordinator of Jean Monnet Module "Online UGhent Academy on EU Law and Policy for Ukrainian Lecturers" (Academy4UA 101085645)

Digital sovereignty is understood as a strategic tool of state development aimed at ensuring security and resilience, strengthening influence on the international political and economic stage, and reducing dependence on high-tech countries [5]. The implementation of digital sovereignty implies that a state must be able to manage digital services and infrastructure while ensuring the protection of citizens' rights and national interests [7]. Digital sovereignty brings together the concepts of geopolitical independence, control over technological infrastructure, economic capacity, and the safeguarding of democratic values and human rights in the field of data and information protection [3].

It should be noted that the concept of digital sovereignty is not yet fully defined and is interpreted differently across countries. For example, the EU focuses on personal data protection and technological independence, aiming to reduce reliance on external IT companies.

Thus, this study aims to identify the key approaches to digital sovereignty in the EU.

Digital sovereignty encompasses four key components:

- data sovereignty – the state's control over the collection, processing, and storage of data within its territory, including the development of regulatory frameworks and the growth of the domestic data market [4];
- technological sovereignty – the ability to independently develop and manage national technologies, including software, hardware, and networks, which is critical for security and innovation [6];
- cybersecurity sovereignty – the capacity to protect digital infrastructure from cyber threats through standards, certification, and effective incident response [1];
- legal sovereignty – the state's right to establish and enforce its own rules in the digital environment, particularly concerning platforms, online services, and e-commerce [5; 3].

Researchers identify four models of digital sovereignty based on values, goals, and descriptive characteristics: Rights-Based Model, Market-Oriented Model, Centralisation Model, and State-Based Model. None of these models provides a perfect balance between regulation and flexibility in responding to technological and social changes. However, each offers valuable guidance for shaping effective policy. The Rights-Based Model seeks to balance fundamental rights and market dynamics but may slow down responses to change. The Market-Oriented Model promotes innovation but often overlooks regulation in sensitive areas. The Centralisation Model enhances control but reduces the involvement of non-state actors and system flexibility. The State-based model shows the potential of government-led innovation, yet its resistance to external influences may lead to internal tensions and institutional inertia. It is important to note that these models are analytical ideal types, and a country may implement elements from several models simultaneously. For example, the EU mostly aligns with the Rights-Based Model, which focuses on protecting democratic values and citizens' rights in the digital environment, balancing user rights with market interests, and involves active regulation of private companies; state control is viewed not as an end in itself, but as a tool to ensure digital freedom, user autonomy, and sovereignty. However, the EU also occasionally employs security-based arguments, such as restricting the presence of certain foreign companies in the internal market [2].

It should be noted that the EU has gradually developed its pursuit of digital sovereignty in response to global technological challenges, advancing initiatives such as the General Data Protection Regulation (hereinafter – GDPR), Digital Services Act (hereinafter – DSA), Digital Markets Act (hereinafter – DMA), Artificial Intelligence Act (hereinafter – AI Act), and Gaia-X, etc. These efforts aim

to protect citizens' rights, support the economy, and promote European values. For example, the Gaia-X project reflects the EU's ambition for technological autonomy, to create a secure European cloud infrastructure to compete with major players from the US and China. The EU regulatory acts – the DSA, DMA, and AI Act – have reshaped the rules for tech giants like Google, Amazon, and Meta by limiting monopolistic practices, enhancing transparency, and strengthening user protection. These measures support the EU's digital sovereignty and compel major companies to adapt their strategies and business models to meet new requirements. For instance, the DMA regulates the behavior of large online platforms ("gatekeepers") to reduce their dominance over competitors. Google has adjusted its search algorithms, while Amazon has changed its approach to promoting its brands. Violations can lead to fines of up to 20% of annual global turnover or even the forced breakup of companies, underscoring the EU's strict regulatory stance. The DSA requires major platforms like Meta and X to combat illegal content and ensure transparency in algorithms and advertising. Violations may result in fines of up to 6% of global turnover. In response, Meta has updated its advertising policy, and X has strengthened its content moderation. These platforms are also investing in AI tools, local teams, and interface redesigns – measures that are more challenging for smaller players but manageable for tech giants. The AI Act is the first attempt to regulate artificial intelligence by classifying systems based on their risk level. High-risk applications, such as facial recognition or automated hiring systems, require companies to ensure transparency, oversight, and responsible data use. This pushes tech giants to adapt their AI products and strategies before entering the EU market. Moreover, EU regulations like the GDPR, DMA, and AI Act have extraterritorial scope – they apply to all foreign companies that handle EU citizens' data or offer them services. As a result, global players like Microsoft and Meta must adjust their services to comply with the EU requirements [3; 2].

However, the implementation of the EU's digital sovereignty strategy faces several challenges. Differences in the level of development among member states and a decentralized digital landscape complicate coordination. Joint actions often require compromises, which can slow down decision-making. Despite aiming to foster innovation, the EU still struggles to compete with technological leaders such as the United States and Asia [3].

As noted in academic literature, the EU needs to strengthen cooperation both at the Union level and among individual member states to distribute resources more effectively and support less developed countries. It is crucial to increase investment in digital infrastructure, particularly through projects like

Gaia-X, to enhance technological independence and competitiveness. Additionally, cybersecurity and data protection must be reinforced by continuing the development of initiatives such as the GDPR and the Cybersecurity Act, which already influence global standards. Investments in AI, blockchain, and other emerging technologies should be accompanied by regulation under the AI Act, combined with funding mechanisms like the Horizon Europe programme. Digital sovereignty is not only about regulation but also about citizen participation. Therefore, it is essential to inform the public about their digital rights. Through initiatives such as the GDPR, DSA, DMA, and AI Act, the EU is laying the foundation for a sustainable and ethical digital space. However, the strategy must remain flexible to adapt to changes and the diverse needs of member states. Striking a balance between national sovereignty and European coordination will enable the EU to become a leader in digital regulation, ensuring security, innovation, and transparency [3].

Thus, the EU's digital sovereignty is a strategic response to the challenges of global digital transformation and increasing dependence on foreign technologies. Its implementation is based on four key pillars: data control, technological autonomy, cybersecurity, and legal regulation. The EU primarily follows the Rights-Based Model, combining the protection of citizens with market mechanisms. The adoption of acts such as the GDPR, DSA, DMA, and AI Act has significantly impacted the operations of global technology companies and contributed to the development of the EU standards for digital governance. At the same time, the implementation of the strategy faces challenges, particularly the uneven development of member states and the complexity of intergovernmental coordination. To achieve full digital sovereignty, the EU must continue investing in infrastructure, innovation, and cybersecurity, while also ensuring active citizen participation. Only a balance between national interests and European coordination will enable the EU not only to protect its digital space but also to become a global leader in digital policy.

The list of used sources:

1. Farrand B., Carrapico H. Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *Eur. Secur.* 2022. Issue 3. P. 435–453. URL: https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2102896#d1e137 (Last Accessed: 21.04.2025).

2. Fratini S. Hine E., Novelli C., Roberts H., Floridi L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *DISO.* 2024.

Volume 3. Issue 59. URL: https://link.springer.com/article/10.1007/s44206-024-00146-7 (Last Accessed: 21.04.2025).

3. Hulkó G., Kálmán J., Lapsánszky A. The politics of digital sovereignty and the European Union's legislation: navigating crises. *Front. Polit. Sci.* 2025. Volume 7. URL: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1548562/full (Last Accessed: 21.04.2025).

4. Hummel P., Braun M., Tretter M., Dabrock P. Data sovereignty: a review. *Big Data Soc.* 2021. *Sage Journals. Big Data & Society.* 2021. Volume 8. Issue 1. URL: https://journals.sagepub.com/doi/epub/10.1177/2053951720982012 (Last Accessed: 21.04.2025).

5. Novikov Ye. Digital sovereignty: conceptual challenges and constitution implications. *Конституційно-правові академічні студії*. 2024. №1. С. 61–69. URL: http://journal-kpas.uzhnu.edu.ua/article/view/311047/302339 (Last Accessed: 21.04.2025).

6. Roumate, F. AI and technological sovereignty. *Artificial Intelligence and the New World Order. New Weapons, New Wars and a New Balance of Power.* Springer Cham, 2024. 165 p. URL: https://link.springer.com/book/10.1007/978-3-031-50312-2 (Last Accessed: 21.04.2025).

7. Suzor N. Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms. *Sage Journals. Social Media + Society.* 2018. Volume 4. Issue 3. URL: https://journals.sagepub.com/doi/epub/10.1177/2056305118787812 (Last Accessed: 21.04.2025).