
*The concept of digital sovereignty in the light of the Constitution
of the Republic of Poland and European Union Law*

Katarzyna CŁAPIŃSKA, Maciej ŁYSZKOWSKI et Maciej MIEDZIEJEWSKI

2026-1, pp. 1-16

Pour citer cet article :

Katarzyna CŁAPIŃSKA, Maciej ŁYSZKOWSKI et Maciej MIEDZIEJEWSKI, « The concept of digital sovereignty in the light of the Constitution of the Republic of Poland and European Union Law », *Jurisdoctoria* 2026-1 [en ligne], *Les Cahiers d'e-Délib* 2025, pp. 1-16

Pour consulter cet article en ligne :

<https://www.jurisdoctoria.net/2026/07/the-concept-of-digital-sovereignty-in-the-light-of-the-constitution-of-the-republic-of-poland-and-european-union-law>

©JURISdoctoria – ISSN 1760-6225

The concept of digital sovereignty in the light of the Constitution of the Republic of Poland and European Union Law

KATARZYNA CŁAPIŃSKA

Student at the University of Warsaw and Paris 1 Panthéon-Sorbonne

MACIEJ ŁYSZKOWSKI

4th law student at the University of Warsaw

MACIEJ MIEDZIEJEWSKI

4th law student at the university of Warsaw

INTRODUCTION

Digitisation is increasingly influencing the way individuals, society and economic and political relations function with each passing year. According to the World Bank, the digital economy accounted for 15% of global GDP in 2022 and is growing much faster than other sectors¹. Corporations operating in this sphere are offering an increasingly wide range of services, from social media² to the provision of high-tech services to the armed forces³. Significantly, US and Asian players

¹ See <https://www.weforum.org/stories/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/> (accessed 08.03.2025).

² Influence through social media can have a very significant impact on state security. The events during the Romanian presidential elections in November 2024 prove this. The Romanian Constitutional Court annulled the first round of the election, pointing out, among other things, that tens of thousands of fake social media accounts were campaigning for the leading candidate. See Constitutional Court Decision No 32 of 6 December 2024 on the annulment of the presidential election (<https://www.ccr.ro/wp-content/uploads/2025/02/RULING-No-32-2024.pdf>). See also the Centre for Eastern Studies' analysis of 09.12.2024: <https://www.osw.waw.pl/pl/publikacje/analizy/2024-12-09/rumunia-sad-konstytucyjny-uniewaznia-wybory-prezydenckie> (accessed 11.03.2025).

³ See, for example, the provision of technology support by Google and Microsoft to the Israel Defence Forces during the Gaza war: <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft> and <https://www.ipost.com/international/article-838681> (accessed 11.03.2025).

are leading the way in this area – there are only two companies from the European Union amongst the top 30 technology companies⁴.

- 2 The growing role of digital services and the necessity to source them from non-EU actors is impactful on the functioning of states. It is essential for countries to have access to the services offered by the technology giants, while at the same time they have no real alternative to obtain them from other actors. The state of dependency is borne out by the figures: around 92% of data in the Western world is stored on servers owned by US companies⁵. Most countries therefore have no way of avoiding contact with these concerns unless they choose to isolate themselves economically and consequently lag behind technologically⁶. Combined with their almost unlimited financial possibilities, these concerns acquire an oligopoly position, which enables them to force countries to make certain decisions.
- 3 Not only states, but also their citizens depend on the services provided by the digital giants for their daily functioning. In doing so, personal data has become a kind of substitute for money – when using digitally provided services (most of which are theoretically free), users continually consent to the processing of their data. Thus, these business entities gain extensive access to information about individuals. This enables insight into their personal and professional lives on an unprecedented scale.
- 4 The phenomena outlined above beg the important question of how effectively EU Member States, as well as the European Union itself, are able to exercise sovereignty over digital service providers on a global scale and how can they become independent of them? The challenge in this area becomes the protection of state sovereignty. It should come as no surprise, therefore, that a relatively new concept of digital sovereignty has been increasingly discussed in recent years at the level of European Union bodies and national governments.
- 5 The debate on digital sovereignty mainly concerns the economic and technological ground. In the legal discourse, this theme has mainly been addressed at the level of public international law and new technology law⁷. The purpose of this publication is to attempt to analyse the issue of digital sovereignty from the perspective of constitutional and EU law, and in particular to assess whether it is possible to

⁴ In terms of stock market capitalisation, these are Germany's SAP and the Netherlands' ASML. See: <https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/> (accessed 08.03.2025).

⁵ Opinion of the European Economic and Social Committee on *Digital Sovereignty: a crucial pillar for EU's digitalisation and growth* (2023/C 75/02, pp. 8-12).

⁶ See also: P. TÜRK, « La "souveraineté numérique" : un concept pertinent en droit constitutionnel ? » in *La souveraineté numérique: le concept, les enjeux*, Mare et Martin 2018, p. 20.

⁷ See more on this issue: P. ROGUSKI, "Suwerenność cyfrowa jako problem badawczy", *Forum Akademickie* 2024, No. 7-8; <https://miesiecznik.forumakademickie.pl/czasopisma/fa-7-8-2024/suwerennosc-cyfrowa-jako-problem-badawczy%E2%80%A9/> (accessed: 27.03.2025); M. ROJSZCZAK, "Suwerenność cyfrowa: budowa strategicznej autonomii w erze globalnych usług cyfrowych", *Państwo i Prawo* 2024, No. 7, pp. 72-103.

read from the Constitution of the Republic of Poland⁸ and define the scope of the obligations of public authorities in the development of digital sovereignty.

I. THE CONCEPT OF DIGITAL SOVEREIGNTY

- 6 The momentousness of the issue at stake is well illustrated by Pierre Bellanger's statement: "sovereignty in a democracy is a collective freedom, a freedom that we decide collectively. It is one of the treasures handed down from generation to generation, and it is the task of each generation to reclaim it by overcoming the challenges of its time. Today, our sovereignty also extends to the digital sphere. Our task, together with our European friends, is to make this additional dimension a new expression of our freedom"⁹.
- 7 Defining digital sovereignty is crucial for further exploration of the concept and its constitutional reading. Its relation to the hitherto established understanding of sovereignty is also important.
- 8 Sovereignty has always been a constitutive factor of the state – Jean Bodin already described it as its fundamental attribute¹⁰. Without it, the state cannot exist as a separate entity and, at the same time, it is the expression of its competence at all levels of functioning. Understood in this way, sovereignty has an external aspect, which is the independence of the state and its authority from external factors, primarily other states. It also has an internal aspect, which is the state's possession of an essentially unlimited monopoly on law-making backed by coercion, which ensures its effective enforcement against subjects subordinate to the state power¹¹.
- 9 Sovereignty in the hereinabove 'classical' sense (and especially its internal aspect) is primarily linked to a given territory and its inhabitants. This makes it possible to precisely define the scope of application of state sovereignty from the material side, i.e. within the boundaries of the territory, and from the subjective side, i.e. according to the nationality or residence of the subject subordinate to the state power.
- 10 The existing concept of sovereignty is being exposed to increasingly serious challenges emerging with increasing digitalisation. This raises questions about the adequacy of the established definition of sovereignty and prompts a rethink. The concept of digital sovereignty may be the answer. As Marcin Rojszczak aptly points out, it is not – contrary to what it may seem – an alternative to the existing sovereignty, but a kind of complement to it¹². To establish a single definition would be simplistic due

⁸ Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws from 1997, No. 78, item. 483).

⁹ P. BELLANGER, « De la souveraineté en général et de la souveraineté numérique en particulier », *Les Échos*, 30 août 2011, https://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm (accessed: 08.03.2025).

¹⁰ H. IZDEBSKI, *Historia myśli politycznej i prawnej*, Warsaw 2013, p. 88.

¹¹ See. J. KRANZ, *Pojęcie suwerenności we współczesnym prawie międzynarodowym*, Warsaw 2015, p. 48 and following.

¹² M. ROJSZCZAK, "Suwerenność cyfrowa" ..., pp. 74-78.

to the multifaceted nature of the concept¹³. For digital sovereignty refers not only to the ability to exercise the competences of power by regulating and enforcing the law not only in a specific territory, but in the digital sphere. It also encompasses the issue of building state and individual sovereignty in cyberspace, which relates primarily to technical and economic issues¹⁴.

- 11 The question of the effectiveness of the exercise of power comes to the fore – whether, in the digital age, it is possible to effectively extend sovereignty also to events in cyberspace. This, in turn, has, over time, ceased to be understood merely as mutually cooperating telecommunications devices and has become an immaterial sphere of interaction between its users¹⁵.
- 12 In this regard, digital sovereignty should be understood primarily as the state's ability to act actively and autonomously in cyberspace through its effective regulation, as well as its ability to effectively protect its digital assets (information and data)¹⁶. The jurisdiction of the state power is assumed to encompass not only the physical information infrastructure in a specific territory, but also the activities in cyberspace concerning the vital interests of the state¹⁷. Pierre Bellanger defines digital sovereignty in this respect as the extension of the state into the immaterial sphere of information that is cyberspace¹⁸. However, it is not sufficient to simply declare sovereignty over it – it is necessary to have concrete technological solutions that are able to ensure the possibility of unfettered action in the digital sphere and the protection of digital assets.
- 13 The above aspect of digital sovereignty is only a component of digital sovereignty, which cannot be implemented without the independent development of technological and economic capabilities. This issue is particularly highlighted in European Union documents¹⁹. This corresponds with the significant problem of the heavy dependence of states and their economic systems on the services provided by global technology companies. The concept of digital sovereignty gains significant importance in this area, as the 'classical' understanding of sovereignty seems inadequate here.

¹³ A review of the various definitions of digital sovereignty is provided by P. TÜRK in: « Définition et enjeux de la souveraineté numérique », *Cahiers français* 2020, No. 415.2, pp. 18-28.

¹⁴ See P. Türk's proposed distinction of three aspects of digital sovereignty: legal, political-economic and individual (« Définition et enjeux... », pp. 23-24).

¹⁵ M. ROJSZCZAK, "Suwerenność cyfrowa...", p. 77.

¹⁶ *Ibid*, pp. 78-81.

¹⁷ See: D. AKANDE, D. HOLLIS (ed.), *The Oxford Process on International Law Protections in Cyberspace: A Compendium*, <https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf> (accessed: 05.04.2025); *Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni* of 29th december 2022 and M.N. SCHMITT, *Tallinn manual 2.0 on the international law applicable to cyber warfare*, Cambridge University Press 2017.

¹⁸ P. BELLANGER, « Souveraineté numérique et ordre public », *Archives de philosophie du droit* 215, No. 58.1, p. 287.

¹⁹ See in particular: *Opinion of the European Economic and Social Committee on Digital Sovereignty...* and Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the "Path to the Digital Decade" policy program for 2030 (OJ L 323, 19.12.2022, pp. 4-26).

- ¹⁴ For this reason, the goal of a digitally sovereign state should be to achieve economic autonomy, which means creating its own technological capabilities that would allow it to self-define its position and effectively perform its activities in cyberspace and the economy. Of particular importance in this regard is scientific and economic investment in digital innovation (cloud computing, artificial intelligence and other technologies), which will guarantee independence from global digital corporations and autonomous control over one's own resources. Attempts are also being made to limit the provision of services by non-EU corporations in strategic areas such as the 5G network²⁰.
- ¹⁵ Digital sovereignty is a multifaceted concept, relating to both the exercise of traditional state competences and a specific digital investment policy. This concept complements the established understanding of sovereignty on further levels and allows an attempt to effectively ensure state autonomy also in the digital age. It is clear from the work already undertaken that digital sovereignty will be exercised primarily at the level of the European Union and not only at the national level.

II. DIGITAL SOVEREIGNTY IN THE LIGHT OF EU LEGISLATION

- ¹⁶ The European Union undertakes numerous efforts to ensure digital sovereignty. These efforts are multidimensional: on one hand, regulating issues related to fundamental rights, including their new dimension due to the technological revolution; on the other hand, striving to provide a number of solutions that influence fair competition in the market among major economic entities. An important and well-developed aspect of the Union's policy is also ensuring security and protection of personal data. Another significant issue in the context of the European Union is regulation concerning artificial intelligence.
- ¹⁷ Starting with the first issue – fundamental rights in the era of new technologies – the Union has made significant efforts, including the adoption of the European Declaration on Digital Rights and Principles in 2023²¹. The third recital of the Preamble states that digital transformation poses a challenge for democratic societies, economies, and citizens. It also emphasized that it cannot be linked to restricting rights and must comply, among others, with personal data protection, the right to privacy, non-discrimination, gender equality, and consumer protection. This approach represents a highly complex project that requires refinement of numerous legal solutions.

²⁰ See Communication from the European Commission: *Implementation of the 5G cybersecurity Toolbox*, <https://digital-strategy.ec.europa.eu/pl/library/communication-commission-implementation-5g-cybersecurity-toolbox> (accessed 10.04.2025). In March 2025 the EC renewed its call to restrict the use of equipment from Huawei. In response to the EC's appeal, the Polish Ministry of Digitalisation announced that it was not planning any action in this direction; <https://businessinsider.com.pl/wiadomosci/ministerstwo-cyfrizacji-brak-planow-zakazu-huawei-w-polskich-sieciach/wnhf1v8> (accessed 10.04.2025).

²¹ Joint Declarations of the European Parliament, Council, and European Commission, *European Declaration of Digital Rights and Principles for the Digital Decade*, 23 January 2023 (OJ C 23, 23.1.2023, pp. 1-7).

- ¹⁸ As for the declaration itself, it includes six chapters, which do not constitute new legal regulations in the strict sense, but represent commitments made by EU bodies in the areas of sustainable development, data control, protection of children and youth in the digital environment, as well as digital education and online training and digital skills.
- ¹⁹ In January 2023, the policy program “Path to the Digital Decade” also came into force. The first recital of the document explicitly states that one of its main goals is the necessity to maintain the digital sovereignty of the European Community. Article 3(1)(c) specifies that this must be done while maintaining openness through secure and accessible digital infrastructure. It also emphasized the need to ensure the storage, transmission, and processing of vast amounts of data.
- ²⁰ The technological revolution has also made fundamental rights – which previously did not often fall within the interest of the public or ordinary citizens – now a top priority. One clear example is the right to personal data protection. The need to prioritize this right today primarily stems from its weight and significance. It is no longer just about securing personal data that could be used for minor economic crimes, but about protecting entire psychological profiles of internet users, which are created to manipulate the electoral process by sending targeted information to influence the choice of a specific candidate.
- ²¹ At this point, one may ask: apart from the declarative nature of the above-mentioned solutions, are there actual regulations and directives that genuinely shape policy?
- ²² The answer is yes. When it comes to ensuring personal data protection, the European Union guarantees a high standard of protection. The General Data Protection Regulation (GDPR)²², adopted in 2016 and enforced after a two-year transition period, represented a practical revolution, particularly in Poland. One of its consequences was the creation of a new body – the President of the Office for Personal Data Protection, which replaced the Inspector General for the Protection of Personal Data. Furthermore, the regulation introduced new rights and obligations. Among the most important, from the perspective of fundamental rights, is the codification of the right to be forgotten²³. First and foremost, it should be emphasized that the right to be forgotten had already existed in EU law, albeit in a less stringent form. Directive 95/46/EC²⁴, whose aim was to harmonize EU regulations across Member States, granted individuals the right to rectify or delete their data held by a data controller²⁵.

²² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, pp. 1–88).

²³ Art. 17(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [GDPR].

²⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ L 281, 23.11.1995, pp. 31–50)

²⁵ Art. 12(b) Directive 95/46/EC.

This issue was also addressed by the Court of Justice of the European Union in Luxembourg in a ruling concerning the processing of data on websites and the responsibility of the search engine operator²⁶. In that ruling, it was justified that, based on the rights enshrined in the Charter of Fundamental Rights, an individual's request for information concerning them to no longer be publicly accessible takes precedence over the economic interests of the search engine operator and the interests of those seeking the information.

- 23 However, the GDPR reinforced the nature of the right to be forgotten in two ways: first, by codifying it at the level of EU regulation, thereby making it directly applicable in national law; and second, by introducing severe penalties for entities that fail to comply with the principles of this regulation²⁷.
- 24 A new challenge to the right to be forgotten has emerged with the development of artificial intelligence, because in order for this right to be fully realized, it is not enough to simply remove information from a search engine – one must also remove all links and copies containing that information.
- 25 The problem with AI is that it not only collects information, but also learns from it and builds its models based on that data. Another issue that arises in this context is the frequent lack of awareness about whether certain personal data has been incorporated into an AI chatbot²⁸.
- 26 Recognizing these issues, the European Parliament has made attempts to codify artificial intelligence. In June 2024, it adopted the Artificial Intelligence Act²⁹, which forms part of a broader legislative package that also covers AI-related innovations, including infrastructure facilitation and a coordinated plan for further development.
- 27 It is important to note that the EU legislator has placed significant emphasis not only on supporting and developing AI economically within the Union but also on ensuring user safety. Among the prohibited practices is the use of emotion analysis for employing subliminal, manipulative, and misleading techniques that distort decision-making processes. An example of this could be the use of AI by shopping centres that have specialized multifunctional systems influencing customer decisions,

²⁶ Judgment of the Court of Justice of the European Union (CJEU) of 13 May 2014, C-131/12, *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317

²⁷ A. SŁAWIŃSKI: “Prawo do bycia zapomnianym” w świetle ogólnego rozporządzenia o ochronie danych osobowych i orzecznictwa TSUE [in:] M. WIĄCEK (ed.) “Prawo do prywatności – współczesne wyzwania”, Warsaw, 2019, pp. 85-90.

²⁸ M. HAPEK, “Asymetria zależności między użytkownikiem a organizacją w dobie sztucznej inteligencji na przykładzie wybranych narzędzi”, *Zarządzanie Mediami*, 2024, No. 12, pp. 17-20.

²⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonized rules for artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019 (OJ L, 2024/1689, 12.7.2024).

such as playing music with words like “buy”, “need”, and “now”, as well as displaying advertisements specifically tailored to the customer based on their credit card transaction history³⁰.

- ²⁸ Special protection has been extended to individuals who are particularly vulnerable due to their age, disability, or economic situation. This refers, for example, to applications functioning as assistants, which collect data and may then display manipulated advertisements encouraging actions such as purchasing specific financial instruments³¹.
- ²⁹ Social scoring has also been prohibited, meaning the classification of individuals based on their behavior if it leads to negative or unfair treatment, as well as profiling a person or assessing their personality to evaluate the risk of committing a crime. This refers to systems that monitor city residents and reward them for “good behavior”. As a result, individuals with a low score could face difficulties finding a job or renting an apartment³².
- ³⁰ The European Union aims to ensure that, on the one hand, regulations protect the fundamental rights of individuals, while on the other hand, they ensure competitiveness in the market. One of the most important challenges of the 2020s will undoubtedly be the rapid emergence of an increasing number of entities that have begun to dominate digital markets.
- ³¹ One of the latest initiatives undertaken by the European Commission was the development of the Digital Markets Act³³, aimed at creating a safe and predictable digital environment based on principles of fairness.
- ³² The most important solution is the introduction of so-called “gatekeepers”, which involves classifying a digital platform as meeting one or more of the following criteria: having a strong economic position with a significant impact on the market, acting as a strong intermediary by connecting many companies, or holding a well-established and durable market position. Once a company is classified as a gatekeeper, it will be subject to obligations, such as allowing its business users to enter into agreements outside of its platform and providing them with data generated by the platform. In the event of non-compliance with these regulations, a platform could face a fine of up to 10% of the company’s total annual turnover, as well as periodic monetary penalties of up to 5% of its average daily turnover. For the first time, the Commission identified six entities as gatekeepers in its decision, including Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft.

³⁰ Ministry of Digitalisation, *Zakazane systemy AI. Analiza rozporządzenia AI Act w zakresie zakazanych praktyk*, prepared by NASK experts, Warsaw 2024, p. 7.

³¹ *Ibid.*, p. 8.

³² *Ibid.*, p. 9.

³³ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (OJ L 265, 12.10.2022, pp. 1-66).

- ³³ In summary, it should be stated that the European Union is taking coordinated actions aimed at protecting digital sovereignty. It accurately identifies emerging threats, such as the need to protect personal data, which has never before been as valuable as it is now, due to the potential for manipulating the entire decision-making process in elections by knowing specific behaviors and preferences of internet users.

III. DIGITAL SOVEREIGNTY IN POLISH POLITICAL AND LEGAL DISCOURSE

- ³⁴ In the broader European context, the digital sovereignty debate in Poland remains relatively underdeveloped and is often characterised by a more defensive and reactive approach. As Marcin Rojszczak notes, Polish public discourse tends to equate digital sovereignty with the protection of critical infrastructure and the affirmation of jurisdiction over the national digital space³⁴. This approach is evident in the official 'Position of the Republic of Poland on International Law in Cyberspace' of 2022, which emphasises the importance of applying existing international law to cyberspace and stresses the state's competence to regulate infrastructure located within national borders³⁵.
- ³⁵ Unlike France or Germany, where digital sovereignty is interpreted as a call for national or European alternatives to foreign technology providers, Poland has so far placed relatively little emphasis on internal technological development or industrial strategy. Instead, the Polish model focuses on legislative control, cyber security enforcement and public administration reforms, including the introduction of cloud services at the national level (national cloud) and projects such as the National Data Processing Centre.
- ³⁶ This differentiation reflects deeper structural and legal assumptions. In the Polish constitutional tradition, sovereignty is primarily associated with territorial jurisdiction and the protection of public authority from external interference. As a result, sovereignty is rarely formulated in terms of technological capabilities. Rojszczak notes that although Poland recognises the importance of cyber security and digital regulation, a comprehensive vision of digital autonomy that combines constitutional obligations with innovative policies is lacking³⁶.
- ³⁷ Moreover, Poland has not developed a unified legal strategy on the implications of digital transformation for sovereignty. Activities are often scattered between different sectors – cyber security, telecommunications, data protection – without a binding constitutional or statutory framework that

³⁴ M. ROJSZCZAK, "Suwerenność cyfrowa...", op. cit.

³⁵ European Commission, *Digital Services Act and Digital Markets Act*, 2022.

³⁶ M. ROJSZCZAK, "Suwerenność cyfrowa...", op. cit.

defines the scope and instruments of digital sovereignty as a state policy objective. This limits the ability of public authorities to coordinate initiatives and influence cross-border digital challenges.

- 38 However, there are perceptible signs of change. The growing awareness of hybrid threats and disinformation campaigns has prompted the Polish authorities to strengthen institutional frameworks such as the Government Plenipotentiary for Cyber Security and the National Cyber Security System. This development reflects a shift towards a more systemic understanding of the digital environment as an area of state interest. Nevertheless, the focus remains on regulation and control rather than proactive development of digital infrastructure and innovation ecosystems.
- 39 From a legal and constitutional perspective, the Polish approach to digital sovereignty remains constrained by traditional understandings of state power. This stands in contrast to emerging European paradigms that place greater emphasis on normative sovereignty – that is, the ability to set standards and frameworks for action in the global digital order. In order for Poland to participate fully in shaping Europe’s digital future, a stronger commitment to the idea of digital sovereignty – one that is based not only on formal jurisdiction, but also on the real possibilities arising from the constitutional obligation to protect national independence, public security and the common good – is necessary³⁷.

IV. CONSTITUTIONAL DUTIES OF PUBLIC AUTHORITIES IN THE CONTEXT OF DIGITAL SOVEREIGNTY

- 40 The development of digital sovereignty is not just a matter of political will or strategic interest – it is increasingly linked to the constitutional obligations imposed on public authorities. In the Polish legal order, the Constitution of 2 April 1997 is the supreme source of law, defining the structure and tasks of the state, the principles of governance and the relationship between public authority and individual rights. Although the term ‘digital sovereignty’ does not appear directly in the text of the Constitution, its various provisions – in particular those concerning the sovereignty of the Republic, national security, the role of public institutions and the protection of the common good – form the normative framework within which digital sovereignty can and should be developed.
- 41 As Marcin Rojszczak emphasises in his analysis, sovereignty in the Polish Constitution has both a symbolic and a functional dimension. Symbolically, Article 4 of the Constitution states that the supreme power in the Republic of Poland belongs to the Nation, exercised directly or through its

³⁷ Chancellery of the Prime Minister, *Krajowy System Cyberbezpieczeństwa – aktualizacja 2023*, Warsaw 2023; (<https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw2>).

representatives. Functionally, the State is obliged to preserve the independence and integrity of its territory (Article 5), ensure the security of its citizens (Articles 26 and 68) and protect the common good (Article 1). These principles, although rooted in the classical paradigm of territorial sovereignty, must today be interpreted in the context of the digital transformation of society³⁸.

- 42 One of the fundamental constitutional duties of public authorities is to protect national independence. In the digital sphere, this means safeguarding the autonomy of decision-making processes, ensuring the resilience of critical digital infrastructure, and minimising dependence on foreign actors that may affect or undermine national interests. This obligation is particularly relevant in light of the dominance of non-European digital service providers in key sectors such as cloud computing, data storage and algorithm-based decision-making. From a constitutional law perspective, reliance on third-party providers without appropriate regulatory controls can be seen as a weakening of sovereignty that requires corrective action by state institutions³⁹.
- 43 Furthermore, digital sovereignty directly intersects with the constitutional principle of state security. Article 26 of the Constitution assigns the Armed Forces the duty to protect the independence and territorial integrity of the Republic. While this duty traditionally referred to physical threats, it now also includes cyber security and the protection of digital infrastructure against hybrid threats, disinformation campaigns and foreign surveillance. Article 68(4), which imposes an obligation on public authorities to counter epidemic threats, should be interpreted similarly – a provision that, as Rojszczak notes, gained a digital dimension during the COVID-19 pandemic, through the management of health data and digital public services⁴⁰.
- 44 Constitutional obligations also arise from Article 74, which imposes an obligation on the state to protect the environment. Although at first glance this provision may seem unrelated, it becomes relevant in the context of the energy and environmental costs associated with digital infrastructure and data centres. A sovereign and constitutionally responsible state should therefore not only regulate digital transformation in the name of control, but also do so with an eye to the principles of environmental sustainability⁴¹.
- 45 Apart from sectoral legislation, the most important normative source supporting digital sovereignty is the general principle of the common good. According to Article 1 of the Constitution, the Republic of Poland is the common good of all citizens. This formulation, although abstract in nature, implies an active role for the state in protecting collective interests, including digital interests. Access to reliable

³⁸ M. ROJSZCZAK, "Suwerenność cyfrowa...", op. cit.

³⁹ B. BANASZAK, "Konstytucja Rzeczypospolitej Polskiej. Komentarz", Warsaw 2021, pp. 132-134.

⁴⁰ *Ibid.*

⁴¹ *Ibid.*

information, protection from surveillance capitalism and immunity from foreign technological manipulation fall directly within the scope of this constitutional obligation⁴².

- ⁴⁶ These obligations are translated into specific tasks for public authorities. Firstly, the state must establish and maintain legal mechanisms capable of effectively regulating the digital space. This includes ensuring that domestic law applies and can be enforced against foreign digital actors operating on Polish territory. The extraterritorial reach of foreign platforms and their growing role in shaping public debate requires a strong domestic regulatory framework that protects the constitutional values of the Republic – in particular pluralism, transparency and accountability.
- ⁴⁷ Secondly, public authorities need to invest in infrastructure to enable national control over data and communications. The development of national cloud solutions, such as the “national cloud”, and data centres, such as the National Data Centre, are examples of attempts to build institutional capacity in line with constitutional objectives. Although these initiatives are still in the early stages of implementation, they signal a shift from a reactive to a proactive approach to building digital sovereignty through public investment⁴³.
- ⁴⁸ Thirdly, public authorities have a constitutional obligation to educate and inform citizens about the risks and rights associated with the digital world. Article 70 of the Constitution guarantees the right to education, while Article 54 ensures freedom of expression and access to information. In the digital age, these provisions imply an obligation to provide citizens with the tools necessary to navigate the digital environment critically and independently. Digital literacy thus becomes not only a matter of educational policy, but also a constitutional imperative⁴⁴. Finally, state bodies need to coordinate their activities at different levels and across different sectors. Currently, as Rojszczak notes, Polish digital sovereignty initiatives are fragmented and lack a coherent legal and strategic framework. The Constitution allows for the creation of special institutions and inter-ministerial coordination mechanisms that could form the basis for a centralised digital sovereignty strategy – provided that these activities are embedded in constitutional values and subject to democratic control⁴⁵.

⁴² *Ibid.*

⁴³ Ministry of Digitalisation, *Założenia Krajowego Centrum Przetwarzania Danych (KCPD)*, Warsaw 2023.

⁴⁴ B. BANASZAK, “Konstytucja Rzeczypospolitej Polskiej...”, *op.cit.*

⁴⁵ *Ibid.*

- ⁴⁹ This interpretation is supported by the jurisprudence of the Constitutional Court, which has consistently emphasised that constitutional principles must be interpreted in a dynamic manner, taking into account changing social and technological realities. A formalistic reading of sovereignty solely as a territorial concept is becoming less and less sufficient. Instead, constitutional interpretation must take into account new areas of state responsibility, including cyberspace, and recognise the state's obligation to ensure autonomy, security and the protection of fundamental rights in the digital context.

V. DIGITAL SOVEREIGNTY AND FUNDAMENTAL RIGHTS

- ⁵⁰ The pursuit of digital sovereignty, while fundamentally rooted in objectives such as state independence, security and regulatory control, inevitably enters the area of fundamental rights and freedoms. In the Polish constitutional order, rights such as freedom of expression, privacy, access to information or protection of personal data are guaranteed in Chapter II of the Constitution. As the state consolidates its position in the digital sphere – through regulation, infrastructure development or taking control of online services – it must do so in a way that respects and protects these rights. The challenge lies in balancing the state's obligation to ensure digital sovereignty with its commitment to respect individual freedom in cyberspace.
- ⁵¹ The Constitution of the Republic of Poland guarantees a broad catalogue of fundamental rights, several of which are particularly relevant in the digital context. Article 47 ensures the right to privacy, Article 49 protects the secrecy of communications, Article 51 regulates the protection of personal data and Article 54 safeguards freedom of expression. These provisions, although adopted before the digital transformation of society, remain relevant in the online environment. As Rojszczak emphasises, the exercise of public authority in the name of digital sovereignty must not violate these rights, but should enhance them through appropriate legal and technical safeguards⁴⁶.
- ⁵² One of the most sensitive areas of this relationship is the regulation of online platforms and digital content. In an effort to assert control over the digital environment and defend national sovereignty, states may be inclined to introduce measures that interfere with freedom of expression online or restrict access to foreign platforms. For example, legislative initiatives in Poland aimed at limiting the influence of 'foreign media' or creating content moderation mechanisms raise concerns about potential abuse and a chilling effect on freedom of expression. As Rojszczak notes, digital sovereignty cannot become an excuse to weaken constitutional guarantees or to impose disproportionate restrictions on freedom of expression⁴⁷.

⁴⁶ Constitution of the Republic of Poland of 2 April 1997, articles 47, 49, 51, 54, 61, 62, 68, 70.

⁴⁷ M. ROJSZCZAK, "Suwerenność cyfrowa...", op. cit.

- ⁵³ At the same time, the digital domain brings with it real threats to individual rights that may justify state intervention. The growing dominance of global technology companies has led to the marketisation of personal data, algorithmic manipulation of content and the erosion of informational self-determination. In this context, digital sovereignty can become a tool for restoring the balance between the individual and transnational corporate power. By regulating platforms, enforcing data protection standards and ensuring the accountability of algorithmic systems, the state fulfils its positive obligations under the Constitution to protect the rights and dignity of citizens.
- ⁵⁴ The dual nature of digital sovereignty – as a tool for empowering citizens, but also as a potential source of constraint – requires that any state action is proportionate, transparent and subject to independent scrutiny. This is particularly relevant in the areas of surveillance and national security. Legal provisions granting public authorities access to digital data or communication content must comply with constitutional standards and be subject to judicial review. The Constitutional Court has repeatedly emphasised that restrictions on rights and freedoms must be based on law, serve a legitimate purpose and respect the essence of the right in question. These principles are of particular relevance when designing legislation on cyber security or extraordinary powers in the digital sphere⁴⁸.
- ⁵⁵ International obligations, including the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union, set additional standards for the protection of privacy, freedom of expression and the protection of personal data. Their validity in the Polish legal order (under Article 91 of the Constitution) further limits the scope of permissible state action. The Polish approach to digital sovereignty must therefore operate within a multi-level system of rights protection in which constitutional and international guarantees complement and reinforce each other⁴⁹. Digital sovereignty also has a positive potential to make rights a reality. By investing in national digital infrastructure, ensuring digital inclusion and secure access to online public services, the state contributes to the realisation of rights such as access to public information (Article 61), the right to education (Article 70) or participation in public life (Article 62). Initiatives such as the national cloud or e-government platforms show that digital capacity building – if properly designed – can increase transparency, efficiency and citizens' sense of empowerment, which are key elements of a democratic constitutional order⁵⁰.
- ⁵⁶ However, Rojszczak warns against instrumentalising digital sovereignty in favour of illiberal agendas. In recent years, some governments – both inside and outside the European Union – have used the rhetoric of 'sovereignty' to justify increased surveillance, censorship or digital isolationism. These tendencies are incompatible with the spirit of the Polish Constitution, which is based on pluralism,

⁴⁸ Constitutional Court Judgment of 12 January 2000, Ref. P 11/98, OTK ZU No. 1/2000, item. 3.

⁴⁹ B. BANASZAK, "Konstytucja Rzeczypospolitej Polskiej...", op.cit.

⁵⁰ *Ibid.*

the rule of law and the inherent dignity of human beings. True digital sovereignty cannot therefore be understood as control for control's sake, but as a constitutional obligation to protect both the state and its citizens in the digital environment⁵¹.

⁵¹ M. ROJSZCZAK, "Suwerenność cyfrowa...", op. cit.

RESUME :

La souveraineté numérique n'est plus un concept abstrait ou uniquement stratégique : elle constitue désormais un élément indispensable de la gouvernance constitutionnelle des États modernes. Dans le cas de la Pologne, le développement de la souveraineté numérique doit être compris non seulement comme un objectif de politique publique, mais également comme une exigence constitutionnelle. Bien que la Constitution polonaise ne fasse pas directement référence à la sphère numérique, ses dispositions relatives à la souveraineté de la République, au rôle des autorités publiques, à la protection des droits individuels et à la poursuite du bien commun établissent un cadre normatif qui justifie, et même impose, l'intervention de l'État dans le domaine numérique. Comme l'a montré cette étude, la compréhension traditionnelle de la souveraineté – fondée sur la compétence territoriale et l'autorité juridique – doit être élargie afin de répondre aux défis et aux opportunités de l'ère numérique. L'émergence des plateformes numériques mondiales, des flux transnationaux de données et des dépendances technologiques contraint les États à affirmer leur présence réglementaire et infrastructurelle au-delà des frontières physiques. Pour la Pologne, cela implique de dépasser une conception défensive de la souveraineté numérique, principalement centrée sur le contrôle des infrastructures, pour adopter une approche proactive fondée sur les valeurs constitutionnelles et une vision stratégique de long terme. L'État polonais – au regard de son mandat constitutionnel – dispose à la fois du droit et du devoir de garantir l'autonomie numérique, de protéger les infrastructures critiques, de soutenir le développement technologique et d'assurer la protection des droits fondamentaux dans la sphère numérique. Ces obligations découlent du principe supérieur du bien commun (article 1), du devoir de protéger l'indépendance et la sécurité nationales (article 5), ainsi que de la garantie des libertés et droits fondamentaux, notamment le droit au respect de la vie privée et la liberté d'expression (articles 47, 49, 51 et 54). Une stratégie de souveraineté numérique tournée vers l'avenir doit donc concilier la puissance de l'État avec les droits individuels, les besoins nationaux avec les standards européens, ainsi que la tradition juridique avec l'innovation technologique. Interprétée et mise en œuvre conformément aux principes constitutionnels, la souveraineté numérique peut devenir un véritable instrument au service de la démocratie : un outil capable de renforcer la résilience de la Pologne, d'accroître la confiance des citoyens envers les institutions numériques et de confirmer la pertinence du droit constitutionnel dans les réalités technologiques du XXI^e siècle.

SUMMARY:

Digital sovereignty is no longer an abstract or solely strategic concept – it is an indispensable element of modern constitutional state governance. In the case of Poland, the development of digital sovereignty should be understood not only as a public policy goal, but also as a constitutional obligation. Although the Polish Constitution does not directly refer to the digital sphere, its provisions on the sovereignty of the Republic, the role of public authorities, the protection of individual rights and the pursuit of the common good create a normative framework that justifies and even requires the state's involvement in the digital sphere. As this article has shown, the traditional understanding of sovereignty – based on territorial jurisdiction and legal authority – must be expanded to meet the challenges and opportunities of the digital age. The emergence of global digital platforms, transnational data flows and technological dependencies requires states to assert their regulatory and infrastructural presence beyond physical borders. For Poland, this means moving away from a defensive model of digital sovereignty focused mainly on infrastructure control, to a proactive model rooted in constitutional values and strategic vision. The Polish state – in light of its constitutional mandate – has both the right and the duty to ensure digital autonomy, protect critical infrastructure, support technological development and guarantee fundamental rights in the digital sphere. These obligations stem from the overriding principle of the common good (Article 1), the duty to protect national independence and security (Article 5) and the guarantee of freedoms and fundamental rights, including privacy and freedom of expression (Articles 47, 49, 51, 54). A future-oriented digital sovereignty strategy must therefore balance state power with individual rights, national needs with European standards, and legal tradition with technological innovation. If interpreted and implemented in accordance with constitutional principles, digital sovereignty can become a tool for democracy – one that will strengthen Poland's resilience, increase citizens' trust in digital institutions and confirm the validity of constitutional law in the realities of 21st century technological development.