

Digital Sovereignty and Constitutionalism in Cyberspace: Challenges for Contemporary Political Institutions

Lecturer **Simona MIHĂILESCU-PENE¹**

Abstract

The accelerated technological transformations of recent decades have generated a profound reconfiguration of the exercise of public power and of the relationships between the state, the citizen, and global private actors. In this context, the concept of digital sovereignty has become central to constitutional and legal debate, reflecting the necessity for states to preserve their regulatory capacity over digital infrastructures, data flows, and emerging technologies. This paper analyzes, from the perspective of constitutional law and the theory of political institutions, the impact of cyberspace on the classical paradigm of sovereignty, as well as the role of political institutions in digital governance. The methodology is based on doctrinal analysis, normative interpretation of relevant constitutional provisions, the comparative method, and the examination of the applicable European legislative framework. The findings highlight the transition from a predominantly territorial sovereignty to a functional one, centered on the control of data and digital infrastructures, as well as the need to adapt constitutional mechanisms to new technological realities. In this respect, the paper advances the thesis that digital sovereignty represents a functional extension of classical constitutionalism. The implications for Romanian legislation consist in the need to strengthen guarantees related to data protection, cybersecurity, and democratic oversight of the use of emerging technologies, in accordance with the principles of legality, proportionality, and the separation of powers.

Keywords: digital sovereignty; constitutionalism; artificial intelligence; fundamental rights; cyberspace; rule of law.

JEL Classification: K10, K24

DOI: 10.62768/PLPA/2026/15/2/02

Please cite this article as: Mihăilescu-Pene, Simona, „Digital Sovereignty and Constitutionalism in Cyberspace: Challenges for Contemporary Political Institutions”, <i>Perspectives of Law and Public Administration</i> 15, no. 2 (June 2026): 205-223.	Article History Received: 18 January 2026 Revised: 15 April 2026 Accepted: 27 May 2026
---	--

1. Introduction

The accelerated development of digital technologies has generated a profound transformation of contemporary legal and political systems, calling into question the fundamental concepts of constitutional law. Among these, the notion of sovereignty occupies a central place, as it defines the capacity of the state to exercise authority and

¹ Simona Mihăilescu-Pene - Faculty of Law, Ecological University of Bucharest, Romania, <https://orcid.org/0000-0002-4060-1965>, simonamihailescu@yahoo.com.

regulate social relations. However, the emergence of cyberspace as a transnational and technologically mediated environment has significantly altered the traditional understanding of sovereignty, requiring its reconceptualization in functional and relational terms.

In classical constitutional theory, sovereignty is intrinsically linked to territoriality and to the monopoly of legitimate authority exercised by the state. The state is conceived as the ultimate source of law, exercising exclusive control over a defined geographical area. However, digitalization disrupts this model by enabling the circulation of data, services, and information across borders in a manner that is difficult to control through traditional legal instruments. This phenomenon is further amplified by the increasingly prominent role of private actors, particularly large technology companies, which exercise significant power over digital infrastructures and information flows.

Within the Romanian constitutional framework, sovereignty is enshrined in Article 2 of the Constitution as belonging to the people and being exercised through representative institutions. At the same time, Article 148 establishes the primacy of European Union law, thereby integrating national sovereignty into a multi-level legal order. This dual framework generates a complex interaction between national constitutional norms and supranational regulatory mechanisms, particularly in the field of digital governance.

The concept of digital sovereignty has emerged as a response to these challenges, reflecting the need of states and supranational entities to strengthen their capacity to control digital infrastructures, data governance, and technological development. However, this concept must be examined with constitutional rigor, as it raises fundamental issues concerning the limits of state power, the protection of fundamental rights and the role of political institutions in regulating cyberspace.

The scientific approach follows two main directions. First, it examines the reconceptualization of sovereignty in the context of digitalization, highlighting the transition from a predominantly territorial sovereignty to a functional one, centered on the control of data and critical infrastructures, as well as the impact of digital technologies on fundamental rights. Second, it analyzes the impact of this transformation on contemporary political institutions, through an assessment of the role of Parliament, the Government, and local public administration authorities in regulating and implementing digital policies.

The paper advances the thesis that digital sovereignty does not represent a rupture from classical constitutionalism, but rather a functional extension thereof, requiring the adaptation of the instruments designed to guarantee the rule of law and the exercise of sovereignty in accordance with the principles of legality, separation of powers and the protection of fundamental rights.

In the absence of an explicit constitutionalization of cyberspace, there is a risk either of a dilution of democratic authority in the face of global technological actors or of excessive regulation with a potentially restrictive impact on fundamental freedoms.

Consequently, the paper argues for the necessity of developing a genuine digital constitutionalism capable of reconciling technological innovation with the

principles of separation of powers, legality, and the protection of fundamental rights.²

2. Research Methodology

The present study adopts a multidisciplinary legal approach, combining several methodological tools specific to constitutional and European law analysis.

First, the doctrinal method is employed to examine both classical theories of sovereignty and contemporary developments in digital constitutionalism. This involves the analysis of Romanian constitutional doctrine, as well as international scholarship addressing the transformation of legal concepts in the digital age. Particular attention is given to the works of Celeste, Bradford, and Kuner, which provide a comprehensive framework for understanding digital sovereignty and its constitutional implications.³

Second, the normative method is used to interpret relevant constitutional provisions, especially Articles 1, 2, 16, 26, and 30 of the Romanian Constitution, in conjunction with European legal instruments.⁴ The interaction between national and European norms is analyzed in order to identify the extent to which digital sovereignty is shaped by supranational regulation.

Third, a comparative method is applied to examine the European model of digital governance and its impact on national constitutional systems. This includes the analysis of the jurisprudence of the Court of Justice of the European Union, particularly in cases concerning data protection and digital rights, such as *Digital Rights Ireland* and *Schrems II*.⁵

Finally, the study incorporates elements of functional analysis, focusing on the role of political institutions in regulating cyberspace and the challenges posed by the emergence of private power. This approach allows for the identification of structural changes in the exercise of public authority and the evaluation of their compatibility with constitutional principles.

² Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* (London: Routledge, 2022), 34, <https://doi.org/10.4324/9781003256908>.

³ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York: Oxford University Press, 2023), <https://doi.org/10.1093/oso/9780197649268.001.0001>; Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013), <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>.

⁴ These include Regulation (EU) 2016/679 (General Data Protection Regulation), Regulation (EU) 2022/2065 (Digital Services Act), Regulation (EU) 2024/1689 (Artificial Intelligence Act), and Regulation (EU) 2022/1925 (Digital Markets Act).

⁵ Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of April 8, 2014, ECLI:EU:C:2014:238, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293>; Court of Justice of the European Union, Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, judgment of July 16, 2020, ECLI:EU:C:2020:559, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>.

3. Digital Sovereignty in Constitutional Theory

Classical Sovereignty and Its Transformation in the Context of Digitalization. The concept of sovereignty has traditionally been defined as the supreme authority of the state, characterized by independence, indivisibility, and territoriality. In classical constitutional theory, sovereignty is closely linked to the notion of state supremacy within a defined geographical space, as articulated by theorists such as Jean Bodin and later developed by Carl Schmitt and Hans Kelsen.⁶

However, this traditional understanding has undergone significant transformation in the context of globalization and European integration. The transfer of competences to supranational institutions, particularly within the European Union, has led to the emergence of a multi-level system of governance in which sovereignty is shared rather than exclusively exercised by the state.

In the Romanian constitutional order, this transformation is reflected in Article 148, which establishes the primacy of EU law. Consequently, sovereignty can no longer be understood as an absolute concept, but rather as a dynamic and functional one, exercised within a network of legal relationships that transcend national borders.

The digital revolution further accelerates this transformation by introducing a domain – cyberspace that is inherently transnational and difficult to regulate through traditional territorial mechanisms. As a result, sovereignty must be reinterpreted as a capacity to regulate digital processes and ensure control over technological infrastructures.

The Emergence and Content of Digital Sovereignty. Digital sovereignty can be defined as the capacity of a state or a political entity to exercise regulatory control over digital infrastructures, data flows, and technological systems in a manner consistent with constitutional principles. Unlike classical sovereignty, it is not strictly territorial but functional, focusing on the ability to influence and regulate digital processes that often transcend national boundaries.

At the European level, digital sovereignty has become a key policy objective, particularly in the context of reducing dependence on non-European technological actors and strengthening strategic autonomy.⁷ The European Union has developed a comprehensive regulatory framework aimed at achieving these objectives, including the GDPR, the Digital Services Act, and the Artificial Intelligence Act.

From a constitutional perspective, digital sovereignty must be understood as a derivative of national sovereignty, subject to the same limitations imposed by the rule of law and the protection of fundamental rights. This implies that the exercise of digital sovereignty cannot justify arbitrary state intervention in cyberspace, but must be grounded in legal norms and subject to judicial review.

The Rise of Private Power and the Crisis of Classical Constitutionalism.

⁶ Carl Schmitt, *Constitutional Theory*, trans. and ed. Jeffrey Seitzer (Durham, NC: Duke University Press, 2008), <https://doi.org/10.1215/9780822390589>.

⁷ European Commission, *Shaping Europe's Digital Future*, COM(2020) 67 final (Brussels, February 19, 2020), 5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067>.

One of the most significant developments in the digital age is the increasing role of private actors in shaping the digital environment. Large technology companies control vast amounts of data, operate critical infrastructures, and influence public discourse on a global scale.

This phenomenon challenges the traditional assumption that constitutional law is primarily concerned with limiting state power. As students have noted, several entities in cyberspace may exercise forms of power that are comparable to those of states, raising questions about accountability and legitimacy.⁸

The concept of “surveillance capitalism,” developed by Zuboff, highlights the extent to which private companies collect and exploit personal data for economic purposes, often without adequate safeguards for individual rights.⁹ Similarly, Bradford emphasizes the emergence of “digital empires,” in which regulatory power is distributed among states.

From a constitutional perspective, this development necessitates a rethinking of the scope of constitutional law. It requires the extension of constitutional principles to private entities, particularly in cases where they exercise significant control over fundamental rights.

Digital Sovereignty as a Constitutionally Limited Concept. While digital sovereignty is often presented as a tool for strengthening state control over cyberspace, it must be understood as a concept that is inherently limited by constitutional principles. The exercise of digital sovereignty must comply with the principle of legality (Article 1(5) of the Romanian Constitution), the protection of fundamental rights, including equality before the law, the right to private and family life, and freedom of expression (Articles 16, 26, and 30), the principle of proportionality in restricting the exercise of rights and freedoms (Article 53(2)), and the principle of the separation and balance of powers (Article 1(4)).

These limitations ensure that digital sovereignty does not become a pretext for excessive state intervention or the erosion of individual freedoms. Thus, digital sovereignty should be conceptualized not as an absolute form of control, but as a constitutionally constrained capacity to regulate digital processes in a manner that balances public interests with individual rights.

4. Fundamental Rights in The Digital Age: Constitutional Reconfigurations and Limits of Digital Sovereignty

The digital transformation of contemporary societies has fundamentally altered not only the modalities through which rights are exercised, but also their very structure and scope. Fundamental rights, traditionally conceived as guarantees against state interference, are increasingly affected by both public and private persons operating in cyberspace. This evolution raises the question whether classical

⁸ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York: Oxford University Press, 2019), <https://doi.org/10.1093/oso/9780190246693.001.0001>.

⁹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), 125.

constitutional frameworks remain adequate to address the complex interplay between technological innovation, private power, and state authority.

From a constitutional perspective, the digital environment introduces a dual challenge. On the one hand, it amplifies the capacity of the state to collect, process, and analyze personal data, thereby increasing the risk of intrusive surveillance. On the other hand, it empowers private entities - particularly large technology companies - to exercise forms of control that directly impact the exercise of fundamental rights. This duality requires a rethinking of constitutional protections in order to ensure their effectiveness in the digital age.

The Right to Privacy and Data Protection: From Individual Guarantee to Structural Principle. The right to privacy, enshrined in Article 26 of the Romanian Constitution, has undergone a significant transformation in the context of digitalization. Traditionally understood as a negative right protecting individuals against arbitrary interference, privacy has evolved into a complex and multidimensional concept encompassing data protection, informational self-determination, and digital identity.

The adoption of the General Data Protection Regulation (GDPR) marked a turning point in the constitutionalization of data protection within the European legal order. The GDPR does not merely regulate data processing; it establishes a normative framework grounded in fundamental rights, particularly Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.¹⁰

This framework introduces principles such as transparency, purpose limitation, and accountability, which aim to rebalance the relationship between individuals and data controllers. However, as noted in doctrine, the effectiveness of these principles is limited by the structural asymmetry between individuals and large digital platforms, which possess both the technological capacity and the economic incentives to process vast amounts of data.¹¹

The jurisprudence of the Court of Justice of the European Union has played a crucial role in reinforcing the constitutional dimension of data protection. In *Digital Rights Ireland*, the Court invalidated the Data Retention Directive, emphasizing that generalized and indiscriminate retention of data constitutes a disproportionate interference with fundamental rights.¹² The Court further clarified that any limitation of the right to privacy must be strictly necessary and proportionate.

This reasoning was extended in *Schrems II*, where the Court invalidated the EU-US Privacy Shield framework, highlighting the inadequacy of protection afforded to European citizens in the context of transatlantic data transfers.¹³ The decision

¹⁰ Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?," *Computer Law & Security Review* 32, no. 2 (2016): 179–194, <https://doi.org/10.1016/j.clsr.2016.02.006>.

¹¹ Kuner, *Transborder Data Flows and Data Privacy Law*, 135.

¹² Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of April 8, 2014, ECLI:EU:C:2014:238, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293>.

¹³ Court of Justice of the European Union, Case C-311/18, *Data Protection Commissioner v. Facebook*

underscored that fundamental rights must be protected not only within the European Union, but also in external data processing contexts, thereby expanding the territorial scope of constitutional guarantees.

In the Romanian context, these developments necessitate a reinterpretation of constitutional provisions on privacy in light of European standards. Article 26 of the Constitution must be read in conjunction with European Union law, resulting in a hybrid model of protection that combines national and supranational norms.

Freedom of Expression and the Rise of Platform Governance. Freedom of expression, protected by Article 30 of the Romanian Constitution, faces unprecedented challenges in the digital environment. While digital platforms facilitate the dissemination of information and enhance democratic participation, they also act as gatekeepers, controlling access to content and shaping public discourse.

This phenomenon has been described as “platform governance,” where private entities establish rules that have normative effects comparable to those of public law.¹⁴ Content moderation policies, algorithmic ranking systems and deplatforming decisions directly impact the exercise of freedom of expression, often without the procedural safeguards associated with state action.

The Digital Services Act (DSA) represents an attempt to address these challenges by imposing obligations on platforms regarding transparency, accountability and due process. However, the regulation of online speech raises complex constitutional questions. As Floridi argues, the risk lies in the emergence of a “privatized censorship,” where decisions affecting fundamental rights are made by private entities without democratic legitimacy.¹⁵

From a constitutional perspective, the key issue is whether and to what extent private platforms should be subject to public law standards. Some students advocate for the horizontal application of fundamental rights, arguing that private entities exercising significant power should be bound by constitutional principles.¹⁶

In Romania, this debate remains largely underdeveloped, but it is likely to gain importance as digital platforms continue to play a central role in public communication.

Artificial Intelligence and the Transformation of Equality and Due Process. Artificial intelligence represents one of the most significant challenges for constitutional law in the digital age. AI systems are increasingly used in decision-making processes that affect individuals’ rights, including credit scoring, recruitment and public administration.

These systems raise serious concerns regarding transparency, accountability, and discrimination. Algorithmic decision-making is often opaque, making it difficult for individuals to understand or challenge decisions that affect them. Moreover, the

Ireland Ltd and Maximillian Schrems (Schrems II), judgment of July 16, 2020, ECLI:EU:C:2020:559, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>.

¹⁴ Cohen, *Between Truth and Power*, 170.

¹⁵ Luciano Floridi, *The Ethics of Information* (Oxford: Oxford University Press, 2013), <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>.

¹⁶ Celeste, *Digital Constitutionalism*, 34.

use of biased datasets may lead to discriminatory outcomes, undermining the principle of equality enshrined in Article 16 of the Romanian Constitution.

The Artificial Intelligence Act introduces a risk-based regulatory framework, distinguishing between unacceptable, high-risk, and low-risk AI systems.¹⁷ High-risk systems are subject to strict requirements, including transparency, human oversight and risk management.

While this approach represents a significant step towards the regulation of AI, it also raises questions regarding its effectiveness. As students have pointed out, the classification of systems and the enforcement of requirements may prove challenging in practice, particularly given the rapid pace of technological development.¹⁸

From a constitutional perspective, the use of AI in public administration requires the development of procedural safeguards to ensure compliance with due process. This includes the right to be informed, the right to contest decisions and the requirement of human oversight.

Towards a Substantive Digital Constitutionalism. The developments analyzed above indicate a broader transformation of constitutional law in the digital age. Fundamental rights are no longer merely defensive instruments protecting individuals against state interference; they have become structural principles guiding the regulation of both public and private power.

This transformation has led to the emergence of digital constitutionalism, a concept that seeks to extend constitutional values into the digital environment.¹⁹ Digital constitutionalism is characterized by: the integration of fundamental rights into technological regulation; the regulation of private power; the development of new accountability mechanisms and the expansion of constitutional guarantees beyond territorial boundaries.

In this context, digital sovereignty must be understood as a constitutionally limited concept. While states have a legitimate interest in regulating cyberspace, this regulation must respect fundamental rights and adhere to the principles of the rule of law.

5. Political Institutions and Digital Governance

Parliamentary Involvement in Digital Transformation. The accelerate technological development poses significant challenges for legislative bodies, which struggle to keep up with innovation. This often results in regulatory gaps or delayed interventions, undermining the effectiveness of legal frameworks.

¹⁷ European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of June 13, 2024, laying down harmonised rules on 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) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2024/1689, July 12, 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

¹⁸ Gianclaudio Malgieri and Frank Pasquale, "Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology," *Computer Law & Security Review* 52 (2024): 105899, <https://doi.org/10.1016/j.clsr.2023.105899>.

¹⁹ Celeste, *Digital Constitutionalism*, 72.

In Romania, this phenomenon is reflected in the increasing reliance on European legislation and executive regulation. While this approach may enhance efficiency, it raises concerns regarding democratic legitimacy and parliamentary oversight.

At the level of constitutional architecture, Parliament remains the primary authority vested with legislative power and democratic legitimacy. In the field of digital governance, its role is essential in establishing the normative framework necessary for the implementation of digital transformation policies and in ensuring the constitutional conformity of such policies.

In Romania, the legislative framework underpinning digital transformation has been progressively developed, particularly in connection with the implementation of the National Recovery and Resilience Plan (PNRR), specifically Component 7 – Digital Transformation. A significant normative step was represented by the adoption of Law no. 242/2022 on the exchange of data between information systems and the creation of the National Interoperability Platform, which aims to facilitate institutional cooperation, reduce administrative burdens and enhance the efficiency of public services.²⁰

Furthermore, the legal framework has been complemented by subsequent legislative developments concerning electronic identification and trust services, including Law no. 214/2024, which consolidates the legal basis for electronic identity instruments such as ROeID and advanced electronic signatures.²¹

However, beyond its formal legislative role, the effectiveness of Parliament in the field of digital governance must be assessed in terms of its capacity to exercise substantive control over the executive. In practice, the accelerated pace of digital reforms, combined with the conditionalities imposed by the PNRR, has led to a relative marginalization of parliamentary deliberation, many key aspects of digital transformation being implemented through executive acts, including Government Emergency Ordinance no. 89/2022.²²

Executive Power and Digital Governance. The executive branch plays a central role in implementing digital policies, particularly in areas such as cyber security, digital infrastructure and public administration.

²⁰ Romania, Law No. 242 of July 20, 2022, on Data Exchange between Information Systems and the Creation of the National Interoperability Platform [*Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate*], *Monitorul Oficial al României*, Part I, no. 752 (July 27, 2022), <https://legislatie.just.ro/Public/DetaliiDocument/257856>.

²¹ Romania, Law No. 214 of July 5, 2024, on the Use of Electronic Signatures, Electronic Time Stamps, and the Provision of Trust Services Based on Them [*Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea*], *Monitorul Oficial al României*, Part I, no. 647 (July 8, 2024), <https://legislatie.just.ro/Public/DetaliiDocument/285178>.

²² Romania, Government Emergency Ordinance No. 89 of June 27, 2022, on the Establishment, Administration, and Development of Cloud-Type IT Infrastructures and Services Used by Public Authorities and Institutions [*Ordonanța de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice*], *Monitorul Oficial al României*, Part I, no. 638 (June 28, 2022), approved with amendments and additions by Law No. 180/2023, as subsequently amended.

In Romania, initiatives such as the governmental cloud and digital public services illustrate the expansion of executive competencies in the digital domain. However, this expansion must remain subject to constitutional constraints, particularly the principles of legality and proportionality.

This is particularly evident in the operationalization of Component 7 of the PNRR. A key instrument in this regard is Government Emergency Ordinance no. 89/2022 on the establishment and use of the governmental private cloud, which lays the legal foundation for the development of a unified digital infrastructure.

The implementation of the governmental cloud has been accompanied by major investments aimed at ensuring interoperability, data integration and the digitalization of public services.

Nevertheless, the centralization of digital governance within the executive raises a series of constitutional concerns. The concentration of decision-making power in the executive and the extensive use of secondary legislation may affect transparency and accountability.²³

Moreover, the development of large-scale digital infrastructures enhances the capacity of the state to collect and interconnect vast amounts of data, raising fears regarding privacy and data protection.²⁴

The executive branch has emerged as the primary actor in digital governance, particularly in areas such as cybersecurity, digital infrastructure, and public administration.

This expansion of executive power raises important constitutional questions. The use of emergency ordinances and secondary legislation in digital regulation may bypass parliamentary scrutiny and affect the balance of powers.

In the Romanian context, this tendency must be carefully monitored, as it may lead to a form of “administrative constitutionalism” in which executive authorities exercise significant normative power.

Obstacles and Structural Challenges. A first major challenge concerns institutional fragmentation and coordination deficits. Organisation for Economic Co-operation and Development (OECD) assessments have highlighted the persistence of silo-based governance and the need for stronger coordination mechanisms.²⁵

A second challenge relates to administrative capacity and implementation speed, particularly in the context of complex digital infrastructure projects.²⁶

Constitutional Risks and Fundamental Rights. A first risk concerns legal certainty and the principle of legality, given the proliferation of normative acts governing digital transformation. A second risk relates to the protection of personal data and privacy, particularly in the context of interoperable systems and centralized

²³ OECD, *Digital Government Review of Romania: Towards a Digitally Mature Government*, OECD Digital Government Studies (Paris: OECD Publishing, 2023), 45, <https://doi.org/10.1787/68361e0d-en>.

²⁴ *Ibid.*, p. 78.

²⁵ OECD, *Digital Government Review of Romania*, 32–40.

²⁶ Authority for the Digitalisation of Romania, *Raportul digitalizării—2025*, accessed March 10, 2026, <https://www.adr.gov.ro/rapoarte-si-studii>.

data infrastructures.²⁷ A third risk concerns equality and access to public services, especially for vulnerable groups affected by rapid digitalization.²⁸

Remedial Directions and Constitutional Safeguards. In light of the constitutional risks identified above, the consolidation of digital governance requires the development of a coherent set of legal and institutional safeguards, capable of reconciling administrative efficiency with the protection of fundamental rights.

A first essential direction concerns the strengthening of the principle of legality and legal certainty in the field of digital governance. Given the proliferation of normative acts regulating digital transformation, it is necessary to ensure a higher degree of legislative coherence and accessibility. This may be achieved through the adoption of comprehensive framework legislation governing digital administration, data governance, and interoperability, thereby reducing reliance on fragmented secondary legislation and emergency ordinances.

A second line of intervention relates to the reinforcement of data protection guarantees. The expansion of interoperable systems and centralized digital infrastructures must be accompanied by stricter safeguards regarding data minimization, purpose limitation, and access control. In addition, the implementation of mandatory audit mechanisms and traceability systems for data access would enhance accountability and ensure compliance with constitutional standards and with the requirements of Regulation (EU) 2016/679.

Thirdly, particular attention must be paid to the protection of fundamental rights in digital administrative procedures. The increasing use of automated processes and digital platforms requires the explicit recognition of procedural guarantees, including the right to be informed, the right to contest administrative decision, and the right to human intervention in cases involving automated decision-making.

A fourth direction concerns the strengthening of parliamentary oversight. In order to preserve the balance of powers, Parliament should exercise a more active role in monitoring the implementation of digital policies, including through periodic evaluations, impact assessments on fundamental rights, and enhanced scrutiny of executive acts adopted in the digital domain.

Fifthly, it is necessary to address the issue of institutional coordination and administrative capacity. The role of the Authority for the Digitalization of Romania (ADR) should be further consolidated, both in terms of legal competences and operational authority, in order to overcome fragmentation and ensure coherence in the implementation of digital policies across public institutions.

Finally, from a broader constitutional perspective, there is a need for the gradual development of a framework of digital constitutionalism, either through legislative refinement or through constitutional jurisprudence. Such a framework should clarify the limits of state intervention in cyberspace, define the applicable

²⁷ European Parliament and Council of the European Union, Regulation (EU) 2016/679 of April 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 (May 4, 2016): 1–88, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

²⁸ OECD, *Digital Government Review of Romania*, p. 102.

standards of proportionality, and ensure that technological innovation remains fully compatible with the principles of the rule of law.

The Role of Courts in Digital Constitutionalism. Courts play a crucial role in ensuring that digital governance complies with constitutional principles. In the absence of comprehensive legislative frameworks, judicial decisions become essential in defining the limits of state and private power.

The jurisprudence of the CJEU demonstrates the importance of judicial oversight in protecting fundamental rights in the digital environment. At the national level, constitutional courts must adapt their interpretative tools to address new technological challenges.

The European Dimension of Digital Sovereignty. The European Union has developed a comprehensive regulatory framework that significantly shapes digital sovereignty.

Key instruments include: GDPR (data protection); Digital Services Act (platform regulation); Digital Markets Act (competition) and AI Act (artificial intelligence).

These instruments reflect a rights-based approach to digital governance, emphasizing the protection of fundamental rights and the regulation of private power.

From a constitutional perspective, this framework contributes to the emergence of a European digital constitutionalism, characterized by the integration of constitutional principles into technological regulation.

However, it also raises questions regarding the balance between national sovereignty and supranational authority, particularly in the context of multi-level governance.

Risks and Constitutional Limits of Digital Sovereignty. Digital sovereignty presents both opportunities and risks. While it enables states to regain control over digital infrastructures, it may also lead to: fragmentation of cyberspace; concentration of power in private operators; excessive state surveillance and erosion of democratic accountability.

6. Artificial Intelligence and Constitutional Limits of Digital Sovereignty

The expedited assimilation of artificial intelligence into both public and private decision-making processes represents one of the most profound challenges for contemporary constitutional law. Unlike traditional administrative or legislative instruments, AI systems operate through complex algorithmic structures that often lack transparency and are difficult to subject to legal scrutiny.

From a constitutional perspective, the use of AI fundamentally alters the relationship between authority and accountability. Decisions that were previously taken by identifiable public officials are increasingly delegated to automated systems, raising serious concerns regarding the principles of legality, transparency and responsibility.

Algorithmic Power and the Erosion of Accountability. One of the defining features of AI is its capacity to process large volumes of data and generate decisions

based on probabilistic models. While this enhances efficiency, it also creates a significant risk of opacity.

In the Romanian constitutional framework, this raises serious issues in relation to Article 1(5), which enshrines the principle of legality. Administrative decisions must be based on clear and predictable legal norms and individuals must have the possibility to understand and contest them. The use of such algorithms may undermine these requirements, leading to a form of “automated governance” that escapes traditional legal control.

Artificial Intelligence and the Principle of Equality. AI systems also pose significant risks in relation to the principle of equality, protected by Article 16 of the Romanian Constitution. Algorithmic bias, resulting from flawed data or design choices, may lead to discriminatory outcomes that are difficult to detect and correct.

Malgieri highlights that algorithmic discrimination is often indirect and systemic, making it more difficult to address through traditional anti-discrimination frameworks.²⁹ This requires the development of new legal instruments capable of addressing structural inequalities embedded in technological systems.

The AI Act attempts to respond to these challenges by introducing strict requirements for high-risk systems, including risk assessment, transparency and human oversight. However, its effectiveness depends on the ability of national authorities to enforce these requirements and to adapt them to specific contexts.

Due Process and the Right to Explanation. The use of AI in decision-making processes raises fundamental questions regarding due process. Individuals affected by automated decisions must have access to effective remedies, including the right to explanation and the right to contest decisions.

The GDPR partially addresses this issue through Article 22, which provides safeguards against solely automated decision-making. However, as Kuner notes, the practical implementation of these safeguards remains limited.³⁰

From a constitutional perspective, due process must be reinterpreted in the digital context, ensuring that procedural guarantees remain effective even when decisions are taken by automated systems.

7. A Personal Doctrinal Perspective: Redefining Digital Sovereignty as Constitutionally Bounded Functional Authority

The analysis conducted throughout this paper supports the conclusion that digital sovereignty cannot be understood as a mere extension of classical sovereignty, nor as a purely political concept reflecting technological autonomy. Instead, it must be reconceptualized as a form of constitutionally bounded functional authority, whose

²⁹ Gianclaudio Malgieri and Cristiana Santos, “Assessing the (Severity of) Impacts on Fundamental Rights,” *Computer Law & Security Review* 56 (2025): 106113, <https://doi.org/10.1016/j.clsr.2025.106113>.

³⁰ Christopher Kuner, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law,” *International Data Privacy Law* 5, no. 4 (2015): 235–245, <https://doi.org/10.1093/idpl/ipv019>.

legitimacy derives not from control over digital infrastructures per se, but from its compliance with fundamental constitutional principles.³¹

In this respect, the prevailing discourse on digital sovereignty, particularly at the European level, tends to emphasize strategic autonomy and technological independence. While these objectives are legitimate, they risk overshadowing the constitutional dimension of digital governance. A sovereignty discourse centered exclusively on control and autonomy may inadvertently legitimize excessive state intervention in cyberspace, potentially undermining fundamental rights.³²

From a constitutional perspective, sovereignty is not an end in itself, but a framework for the exercise of public power within the limits imposed by the rule of law. Consequently, digital sovereignty must be evaluated not by the extent of control it enables, but by the degree to which it preserves constitutional guarantees.³³

Digital Sovereignty Beyond the Logic of Control. A key doctrinal clarification proposed in this paper is the rejection of a purely control-based understanding of digital sovereignty. The ability of the state to regulate data flows or digital infrastructures should not be equated with the expansion of sovereignty in a constitutional sense.³⁴

Rather, digital sovereignty should be understood as the capacity to ensure: the effective protection of fundamental rights in the digital environment; the accountability of both public and private entities and the preservation of democratic legitimacy in technologically mediated governance.

This approach shifts the focus from sovereignty as power to sovereignty as responsibility, aligning the concept with the normative foundations of constitutional law.³⁵

The Constitutionalization of Private Power: A Necessary Evolution. One of the central arguments advanced in this paper is that the rise of private actors in cyberspace requires a reconfiguration of constitutional theory. Traditional constitutionalism is primarily concerned with limiting state power; however, in the digital environment, private entities exercise forms of power that may have an equivalent or even greater impact on fundamental rights.³⁶

In this context, the extension of constitutional principles to private sector becomes not only desirable, but necessary. This does not imply a direct transposition of public law obligations onto private entities, but rather the development of hybrid regulatory frameworks that ensure: transparency of algorithmic systems; procedural safeguards in content moderation; and accountability mechanisms for data processing.

³¹ Celeste, *Digital Constitutionalism*, 45.

³² Bradford, *Digital Empires*, 52–60.

³³ Ernst-Wolfgang Böckenförde, *Constitutional and Political Theory: Selected Writings*, vol. 1, ed. Mirjam Künkler and Tine Stein, trans. Thomas Dunlap (Oxford: Oxford University Press, 2017), 89, <https://doi.org/10.1093/acprof:oso/9780198714965.001.0001>.

³⁴ Kuner, *Transborder Data Flows and Data Privacy Law*, 110–115.

³⁵ Luigi Ferrajoli, *Principia iuris: Teoria del diritto e della democrazia*, vol. 1, *Teoria del diritto* (Roma-Bari: Laterza, 2007), 312.

³⁶ Cohen, *Between Truth and Power*, 120–135.

Such an approach reflects a broader transformation of constitutional law, from a state-centered model to a networked model of governance, in which multiple actors are subject to constitutional constraints.³⁷

Artificial Intelligence and the Limits of Automation in Public Authority. A further doctrinal position advanced here concerns the limits of automation in the exercise of public authority. While artificial intelligence offers significant advantages in terms of efficiency and predictive capacity, its use in decision-making processes must be strictly limited by constitutional guarantees³⁸.

In particular, the delegation of decision-making powers to algorithmic systems must not lead to the erosion of: individual accountability; procedural transparency or to the right to effective judicial protection.

In this sense, the principle of human oversight should be elevated to a constitutional requirement in cases where AI systems are used in public administration.³⁹

Digital Sovereignty in the Romanian Constitutional Context. From the perspective of Romanian constitutional law, digital sovereignty must be interpreted in light of Articles 1(5), 16, 26, and 30 of the Constitution, as well as Article 148 concerning the relationship with EU law.

This implies that digital regulation must comply with the principle of legality and legal certainty; fundamental rights must be effectively protected in the digital environment and European legal standards must be integrated without undermining constitutional identity.

In practical terms, this requires a more active role for national institutions, particularly Parliament and the Constitutional Court, in shaping digital governance.⁴⁰

8. Conclusions

Digital sovereignty represents a structural transformation of the classical concept of sovereignty, generated by the transition from territorial forms of authority to functional and technologically mediated forms of governance. In cyberspace, the effectiveness of state authority no longer depends exclusively on the capacity to control a geographically defined territory, but increasingly on the ability to regulate data flows, digital infrastructures, algorithmic systems, and transnational technological actors. This transformation does not render classical sovereignty obsolete. Rather, it requires its reinterpretation in accordance with the realities of a legal and political order in which authority is exercised simultaneously at national, European, and private levels.

³⁷ Cohen, *Between Truth and Power*, 120–135.

³⁸ Gianclaudio Malgieri, “Automated Decision-Making in the EU Member States: The Right to Explanation and Other ‘Suitable Safeguards’ in the National Legislations,” *Computer Law & Security Review* 35, no. 5 (2019): 105327, <https://doi.org/10.1016/j.clsr.2019.05.002>.

³⁹ Ioan Muraru and Elena Simina Tănăsescu, eds., *Constituția României: Comentariu pe articole* (Bucharest: C.H. Beck, 2008), 35–60.

⁴⁰ Celeste, *Digital Constitutionalism*, 45.

The analysis conducted in this paper demonstrates that digital sovereignty cannot be understood as an unlimited power of the state to control technological infrastructures or information flows. In a constitutional democracy, it must be conceived as a form of constitutionally bounded functional authority. Its legitimacy derives not merely from the pursuit of technological autonomy or strategic independence, but from compliance with the rule of law, the separation and balance of powers, the protection of fundamental rights, and the requirements of necessity and proportionality. Consequently, the expansion of the state's technological capacity must be accompanied by an equivalent strengthening of legal safeguards, democratic oversight, and judicial review.

From the perspective of the Romanian constitutional order, the exercise of digital sovereignty must comply with the principle of legality and legal certainty established by Article 1(5) of the Constitution, the separation and balance of powers provided for in Article 1(4), the principle of equality enshrined in Article 16, the protection of private and family life under Article 26, freedom of expression under Article 30, and the proportionality requirements applicable to restrictions on fundamental rights under Article 53. These constitutional provisions must also be interpreted in conjunction with Article 148 of the Constitution and with the European regulatory framework governing data protection, digital services, digital markets, and artificial intelligence. Digital sovereignty therefore operates within a system of multilevel constitutionalism in which national authority, European Union law, and European fundamental-rights standards are mutually interconnected.

A central conclusion of the study is that contemporary constitutionalism must address not only the exercise of public power, but also the growing normative and infrastructural power of private technological actors. Digital platforms, cloud-service providers, data intermediaries, and developers of artificial intelligence systems increasingly influence access to information, public discourse, economic opportunities, and the exercise of individual rights. Their decisions may produce effects comparable to those traditionally associated with public authorities, even though such decisions are often adopted without the guarantees of transparency, legality, impartiality, and due process that characterize state action. Digital constitutionalism must therefore develop mechanisms capable of ensuring the accountability of private actors, particularly where their activities affect fundamental rights or essential digital infrastructures.

Artificial intelligence illustrates with particular clarity the need to adapt constitutional guarantees to technological decision-making. The use of algorithmic systems by public authorities may improve administrative efficiency, consistency, and predictive capacity, but it may also produce opacity, discrimination, and a diffusion of legal responsibility. Public authorities cannot transfer their constitutional responsibilities to technological systems. Where automated tools are used in administrative decision-making, individuals must retain the right to be informed about their use, to understand the essential grounds of decisions, to challenge their outcomes, and to obtain meaningful human review. Human oversight should therefore be regarded not merely as a technical or ethical requirement, but as an essential

constitutional safeguard whenever algorithmic decisions may significantly affect individual rights or legal interests.

The institutional dimension of digital sovereignty is equally important. Parliament must retain a substantive role in defining the legal framework of digital transformation and in scrutinizing executive policies concerning digital infrastructures, cybersecurity, interoperability, data governance, and artificial intelligence. Excessive reliance on emergency ordinances, secondary legislation, or technically opaque administrative measures may weaken democratic deliberation and disturb the constitutional balance between legislative and executive authority. Parliamentary oversight should include periodic assessments of digital policies, fundamental-rights impact assessments, transparency obligations, and effective mechanisms for holding public authorities accountable for the design and operation of large-scale digital systems.

At the executive and administrative levels, the digitalization of public services should be accompanied by clearer institutional competences, stronger coordination, and adequate administrative capacity. The development of interoperable databases and centralized digital infrastructures creates significant opportunities for improving public administration, but also intensifies risks concerning privacy, data security, unauthorized access, and the concentration of informational power. These risks require strict compliance with the principles of data minimization, purpose limitation, cybersecurity, traceability, and access control. Mandatory technical and legal audits should become an integral component of digital governance, rather than an exceptional response to technological failure or rights violations.

Courts, including the Constitutional Court, administrative courts, and ordinary courts, will have a decisive role in defining the practical limits of digital sovereignty. Judicial review must remain effective even where public decisions are based on technically complex systems or on algorithmic assessments that are difficult to explain. Courts should be capable of examining not only the formal legal basis of digital measures, but also the functioning, proportionality, and rights-related consequences of the technological systems through which public power is exercised. In this regard, constitutional and judicial interpretation will be essential for transforming general constitutional principles into effective safeguards applicable to digital environments.

The European Union's regulatory model provides an important framework for this development by linking technological regulation with fundamental-rights protection and the accountability of powerful digital actors. Nevertheless, the effectiveness of this framework depends on its coherent implementation by national institutions. European regulation cannot substitute entirely for domestic democratic deliberation, administrative capacity, or constitutional review. Romania must therefore develop its own coherent approach to digital governance, consistent with European law but responsive to the institutional, administrative, and constitutional characteristics of the national legal order.

Ultimately, digital sovereignty should not be assessed according to the quantity of data controlled by the state, the degree of technological centralization

achieved, or the extent of dependence reduced in relation to foreign technological actors. Its constitutional value should be measured by the ability of the legal system to preserve human dignity, individual autonomy, equality, freedom of expression, privacy, democratic legitimacy, and effective judicial protection in technologically mediated environments. Digital sovereignty must therefore be understood as sovereignty exercised through responsibility, accountability, and constitutional restraint.

Digital constitutionalism offers the normative framework necessary for achieving this objective. It does not oppose technological innovation, nor does it seek to preserve legal institutions in an unchanged form. Instead, it requires innovation to be integrated into a constitutional order capable of controlling both public and private power. The principal challenge for contemporary political institutions is thus not merely to become technologically capable, but to ensure that technological capability remains legally limited, democratically legitimate, institutionally accountable, and oriented towards the protection of the individual. Only under these conditions can digital transformation strengthen, rather than undermine, constitutional democracy.

Bibliography

1. Böckenförde, Ernst-Wolfgang. *Constitutional and Political Theory: Selected Writings*. Vol. 1. Edited by Mirjam Künkler and Tine Stein. Translated by Thomas Dunlap. Oxford: Oxford University Press, 2017. <https://doi.org/10.1093/acprof:oso/9780198714965.001.0001>.
2. Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology*. New York: Oxford University Press, 2023. <https://doi.org/10.1093/oso/9780197649268.001.0001>.
3. Celeste, Edoardo. *Digital Constitutionalism: The Role of Internet Bills of Rights*. Abingdon: Routledge, 2022. <https://doi.org/10.4324/9781003256908>.
4. Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York: Oxford University Press, 2019. <https://doi.org/10.1093/oso/9780190246693.001.0001>.
5. De Hert, Paul, and Vagelis Papakonstantinou. "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" *Computer Law & Security Review* 32, no. 2 (2016): 179–194. <https://doi.org/10.1016/j.clsr.2016.02.006>.
6. European Commission. *Shaping Europe's Digital Future*. COM(2020) 67 final. Brussels, February 19, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067>.
7. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of April 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L 119 (May 4, 2016): 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
8. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of June 13, 2024, Laying Down Harmonised Rules on 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) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of*

- the European Union L 2024/1689, July 12, 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.
9. Ferrajoli, Luigi. *Principia iuris: Teoria del diritto e della democrazia*. Vol. 1, *Teoria del diritto*. Roma-Bari: Laterza, 2007.
 10. Floridi, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2013. <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>.
 11. Kuner, Christopher. "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law." *International Data Privacy Law* 5, no. 4 (2015): 235–245. <https://doi.org/10.1093/idpl/ipv019>.
 12. Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013. <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>.
 13. Malgieri, Gianclaudio. "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations." *Computer Law & Security Review* 35, no. 5 (2019): 105327. <https://doi.org/10.1016/j.clsr.2019.05.002>.
 14. Malgieri, Gianclaudio, and Frank Pasquale. "Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology." *Computer Law & Security Review* 52 (2024): 105899. <https://doi.org/10.1016/j.clsr.2023.105899>.
 15. Malgieri, Gianclaudio, and Cristiana Santos. "Assessing the (Severity of) Impacts on Fundamental Rights." *Computer Law & Security Review* 56 (2025): 106113. <https://doi.org/10.1016/j.clsr.2025.106113>.
 16. Muraru, Ioan, and Elena Simina Tănăsescu, eds. *Constituția României: Comentariu pe articole*. Bucharest: C.H. Beck, 2008.
 17. Romania. Government Emergency Ordinance No. 89 of June 27, 2022, on the Establishment, Administration, and Development of Cloud-Type IT Infrastructures and Services Used by Public Authorities and Institutions [*Ordonanța de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice*]. *Monitorul Oficial al României*, Part I, no. 638, June 28, 2022. Approved with amendments and additions by Law No. 180/2023, as subsequently amended.
 18. Romania. Law No. 242 of July 20, 2022, on Data Exchange between Information Systems and the Creation of the National Interoperability Platform [*Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate*]. *Monitorul Oficial al României*, Part I, no. 752, July 27, 2022. <https://legislatie.just.ro/Public/DetaliiDocument/257856>.
 19. Romania. Law No. 214 of July 5, 2024, on the Use of Electronic Signatures, Electronic Time Stamps, and the Provision of Trust Services Based on Them [*Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea*]. *Monitorul Oficial al României*, Part I, no. 647, July 8, 2024. <https://legislatie.just.ro/Public/DetaliiDocument/285178>.
 20. Schmitt, Carl. *Constitutional Theory*. Translated and edited by Jeffrey Seitzer. Durham, NC: Duke University Press, 2008. <https://doi.org/10.1215/9780822390589>.
 21. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.