Sovereignty in the Digital Age: From Territorial Authority to Networked Power in Global Politics

السيادة في العصر الرقمي: من السلطة الإقليمية إلى القوة الشبكية في السياسة العالمية

BEN MESSAHEL Alaerrahmane
M'sila University
Laboratory of New Political Sciences
Alaerrahmane.benmessahel@univ-msila.dz

Date of Submission 02-04-2026 Date of Final Acceptance 19-05-2026 Date of Publication June 2026

Abstract:

The digital transformation has fundamentally altered the core principles of sovereignty within contemporary global politics. As cyberspace, data flows, and digital infrastructures extend beyond territorial boundaries, conventional understandings of sovereignty—rooted in territorial control and exclusive authority—are increasingly challenged. This article investigates the ways in which digital transformation redefines sovereignty by introducing the concept of digital sovereignty as a multidimensional and contested form of power. Employing a descriptive-analytical methodology, the study traces the conceptual evolution of sovereignty, identifies the principal actors and dimensions of digital sovereignty, and examines the primary political, legal, economic, and security challenges confronting it. The analysis contends that digital sovereignty is not simply a continuation of traditional sovereignty; rather, it signifies a qualitative transformation in the exercise of power, authority, and control within the digital era. The article concludes that states must adopt adaptive and cooperative governance strategies to balance technological innovation, national interests, and individual rights in an increasingly interconnected global system.

Keywords: Sovereignty, Digital Age, Digital Sovereignty, Digital Humanity, Global Challenges.

ملخص:

في ظل التوترات الجيوسياسية المتزايدة، والحروب، والتحديات العالمية مثل تغير المناخ، والأوبئة، والجرائم الإلكترونية، وهيمنة شركات التكنولوجيا العالمية، تعرض مفهوم السيادة التقليدية، كما صاغه جان بودان، لتحولات عميقة. يركز المقال على دراسة السيادة المتنازع عليها في العصر الرقمي، حيث يبدأ بتناول العلاقة بين التكنولوجيا الرقمية والسيادة الوطنية في سياق النظام الدولي. يهدف المقال إلى استكشاف تأثير التكنولوجيا على استقلال الدول الاستراتيجي، وتحليل التحديات التي تواجه تطوير سياسات عامة فعّالة للتعامل مع قضايا السيادة الرقمية. كما يسعى إلى تسليط الضوء على الأشكال المرغوبة والممكنة للسيادة في العصر الرقمي، مع فهم التفاعل المعقد بين التكنولوجيا والمجتمع. يبرز المقال أهمية معالجة قضايا الجيوسياسية والسيادة ضمن إطار الإنسانية الرقمية، باعتبارهما عنصرين أساسيين في تشكيل المستقبل الرقمي للعالم.

الكلمات المفتاحية: السيادة، العصر الرقمي، السيادة الرقمية، الإنسانية الرقمية، التحديات العالمية.

*** Corresponding Author: BEN MESSAHEL Alaerrahmane.**

Introduction:

The international order currently faces significant disruption, marked by a range of cross-border threats including geopolitical conflicts, the disruptive influence of digital technologies and large technology companies, as well as global challenges such as cybercrime, pandemics, and climate change. Within the digital realm, the traditional notion of sovereignty is no longer applicable, giving rise to the utilization of technology to reinforce sovereignty—whether for states or individuals—enabling a form of global citizenship that transcends geographical boundaries and state control. Consequently, digital sovereignty has become a crucial issue in modern global politics, reflecting both the challenges and opportunities encountered by states in the information age. The significance of digital sovereignty continues to grow alongside the increasing reliance on digital technologies, with the protection of personal data and national information assuming paramount importance. States are under mounting pressure to safeguard citizens' data against violations and breaches.

This article employs a critical geopolitical approach inspired by John Agnew's critique of the territorial trap, positing that digital sovereignty is neither the end of sovereignty nor merely its extension, but rather a reconfiguration of power across both territorial and networked domains. By integrating insights from political geography and international relations, the article situates digital sovereignty as a fundamental mechanism through which power is exercised, challenged, and redistributed in contemporary global politics.

The rapid advancement of technology and the ongoing digital transformation have elevated digital sovereignty to a pivotal issue within global politics. Traditional concepts of sovereignty, formerly anchored in the geographical boundaries of the state, have evolved into more complex notions related to data, cyberspace, and technological control. In this context, the central question addressed by the study emerges:
How does digital transformation influence the concept of sovereignty in global politics?

To address this primary issue, the study raises the following sub-questions:

- What is the impact of digital transformation on global politics?
- How has the concept of sovereignty evolved from its traditional definition to that of digital sovereignty?
- What are the analytical dimensions of digital sovereignty? What are the principal challenges confronting digital sovereignty in global politics?

Descriptive-analytical approach: This methodology is employed to examine the process of digital transformation and its repercussions for global politics, as well as to investigate the various dimensions of digital sovereignty.

The objectives of the study are as follows:

- Analyze the impact of digital transformation on global politics.
- Explain the conceptual transition of sovereignty from its traditional form to a digital one.
- Highlight the analytical dimensions of digital sovereignty.
- Discuss the principal challenges facing digital sovereignty and propose viable solutions to address them.

This article contributes to the literature on sovereignty and digital politics by conceptualizing digital sovereignty as a hybrid form of power that merges territorial authority with network-based control. In contrast to studies that approach digital sovereignty solely as a technical or regulatory matter, this

paper frames it as a geopolitical and normative transformation. This transformation reshapes state authority, redistributes power among state and non-state actors, and challenges the classical Westphalian model of sovereignty.

Accordingly, this article does not merely describe digital sovereignty; it analytically demonstrates how digital sovereignty functions as a hybrid regime of authority, reshaping state power, legitimizing new actors, and transforming the spatial foundations of sovereignty beyond the Westphalian paradigm.

Section I: The Impact of Digital Transformation in Global Politics.

In this section, the impact of digital transformation on global politics is addressed by focusing on the transition in the concept of sovereignty.

A) The Shift to Digital Sovereignty in Global Politics

In response to the emerging challenges states encounter within cyberspace, calls have arisen advocating that national governments lack genuine sovereignty in cyberspace, prompting them to adopt policies aimed at establishing digital sovereignty.

1. Factors of Shift:

Factors such as the rise of multinational corporations, the development of global communication infrastructures, international or regional treaties, and global challenges like pandemics can restrict the extent of sovereign authority[1].

The growing emphasis on the geo-economic and geopolitical aspects of digital policymaking has heightened this challenge, as states increasingly seek to protect and strengthen digital governance. This has driven a reconsideration of the foundational terms of the sovereignty debate, shaped by negotiations and reinterpretations of political authority in complex and spatially diverse ways. According to modern political theory, the world is organized into interconnected geographical units, with the territorial state serving as the fundamental building block from which other territorial entities originate or evolve. As John Agnew posits, "sovereignty is neither territorial in nature nor is it organized exclusively on a state-by-state basis."

Moreover, the Internet has had a profound effect on the role of sovereignty, amplifying its complexities. The problem does not stem from a lack of clarity about "sovereignty," but from the inherent contradiction between traditional power and electronic power. The exclusive control and authority that define political sovereignty cannot be seamlessly applied to the ever-evolving global cyberspace constructed by the Internet. The Internet operates based on software protocols whose origins are not owned by any single entity, and exclusive control cannot be exercised by any actor. Digital sovereignty is at odds with the division of international trade associated with the production of information technology software that has emerged since the 1990s[2].

Within this context, the digital revolution offers a framework for reevaluating and reimagining the modern conception of sovereignty, suggesting that the territorial organization of political entities is not a necessity[3].

2. Framework of Digital Sovereignty:

Accordingly, Daniel Philpott identifies three foundational principles upon which the modern notion of sovereignty rests[4]:

- The sovereign possesses authority.
- The sovereign holds supreme authority.
- Territoriality serves as the ultimate component of sovereignty.

The idea of digital sovereignty assumes a "strategic autonomy" that aims to make the state a "digital power," another similarity to the idea of modern sovereignty as it emphasizes authority and the exclusive concept of identity and territoriality.
According to John Agnew, the reinterpretation and negotiation of political power in complex and spatially diverse ways necessitate a reassessment of the framework through which sovereignty is discussed. Postmodernist perspectives question the contemporary relevance of sovereignty, often critiquing it as a concept deeply rooted in Western traditions of imperialism and colonialism. The modernist understanding of sovereignty has therefore faced various forms of scrutiny and criticism[5].
It is difficult to maintain an absolute position on sovereignty in the face of global interconnectedness. Within the context of increasing global interconnectedness, maintaining an absolute and static position on sovereignty has become increasingly difficult. Sovereignty within digital environments does not equate to isolationism or self-enclosure; rather, it is associated with the call for a "shared, free, open, and secure global internet." As such, digital sovereignty has emerged as a guiding principle for navigating this new landscape. Couture and Tobin observe that, "while digital sovereignty may be somewhat fashionable and useful today, many of the issues discussed are often approached without reference to colonialism, imperialism, and a critique of sovereignty itself. The question, then, is: what is to be gained and what is to be lost in the use of sovereignty when thinking about digital sovereignty?"[6]

Within this framework, digital sovereignty incorporates the notion that multiple agents may exercise sovereignty concurrently as "actors," indicating that sovereignty itself can be distributed and shared. For instance, corporations such as Facebook, alongside national governments, are actively redefining what it means for an entity to possess and exercise sovereignty, through a continual process of interaction and balancing[7].

Consequently, digital sovereignty should not be understood as defined by rigid or fixed boundaries. Instead, it should be conceived as something that can be exercised across political communities and spatial networks extending beyond the confines of the nation-state. Nevertheless, digital sovereignty is not entirely divorced from the traditional concept of sovereignty. It remains fundamentally concerned with "states defending their strategic interests, affirming their values, maintaining consistency in their objectives, and possessing confidence in their means."[8]

This perspective, employed by officials engaged in "practical geopolitics," as well as think tanks, leading scholars, and individuals, has contributed to the emergence of "popular geopolitics" as a recognized discourse.

B) The impact of digital transformations on the concept of sovereignty:

Significant changes and transformations in the concept of sovereignty have arisen due to digital technologies, among which the following are particularly notable:

1. The Territorial Dimension of Sovereignty:

In the digital era, novel digital factors have surfaced, including national digital identity, digital space, national, regional, and civil domain names, national health data, and digital twins of domestically produced goods or smart cities. Additionally, the notion of cyberspace encompasses a complex amalgamation of digital assets such as servers, data centers, and local digital networks, each possessing a physical location and thus falling within sovereign jurisdictions. This physical infrastructure is complemented by transnational networks, as well as non-material standards, protocols, and digital services. Alongside these digital factors, traditional geographic space continues to underpin the classical conception of sovereignty. Collectively, these digital developments are driving an expansion in the scope of sovereign space in the digital age. States lacking a coherent concept of digital territory now face the risk of losing valuable resources. To prevent digital

technologies from eluding traditional territorial sovereignty, many states have adopted data localization measures, resulting in technological architectures characterized by embedded digital borders[9].

2. The Institutional Dimension of Sovereignty:

The institutional dimension of sovereignty is significantly shaped and defined by digital technology. Digital innovations provide unprecedented opportunities for states to access information about citizens and engage with them directly. This transformation encompasses a wide spectrum—from the delivery of intelligent, streamlined, and efficient public services such as child benefits, permits, and voting, to the more problematic scenarios of governmental surveillance and comprehensive social registration. Digital technologies can challenge and even render obsolete traditional models of institutional sovereignty. It is not solely government authorities that are reshaping institutional architectures in response to digital advancements. Certain institutional frameworks, particularly legal systems, struggle to function effectively when reliant on autonomous artificial intelligence, especially in the context of responding to rapidly evolving cyber-attacks driven by artificial intelligence. In some instances, the reverse may occur: traditional models of sovereignty persist, adapting technology to serve established frameworks. For example, rather than relying on open, global blockchain systems, permissioned distributed ledger technologies have emerged, allowing specific groups—such as national customs administrations—to maintain authority and oversight, while still benefiting from the efficiencies associated with more open systems[10].

Despite these developments, there remains no comprehensive technological solution to the challenges posed by autonomous AI that would guarantee continued human oversight and uphold political accountability, a fundamental pillar of domestic legitimacy. This situation creates a profound dilemma: while reliance on autonomous AI may become essential to preserve sovereignty, such dependence could ultimately undermine the very foundation of sovereignty over time.

Section II: The conceptual transition of sovereignty: from traditional to digital sovereignty.

The digital revolution of the twentieth century catalyzed a fundamental reconsideration of sovereignty and the conduct of states within the context of digitized politics and international relations. This transformation challenged the state's ability to withstand breaches of sovereignty. With the proliferation of global digital networks and the surge of digital applications and communication practices in the 1990s, the notion of the state's disappearance became an immediate and plausible scenario. This led to the emergence of the concept of digital sovereignty in recent years, reaffirming state authority and intervention within the digital domain. Digital sovereignty has become a potent concept within political discourse, aimed at reviving and restoring the role of the nation-state.

Traditionally, sovereignty connotes that states possess autonomy in the management of their internal affairs, mandating mutual respect for sovereignty among countries. This, however, represents a simplified, idealized view of sovereignty. While sovereignty pertains to the organization of power within society—particularly the relationship between citizens and the state—digital sovereignty extends these principles into the digital realm. State sovereignty is typically defined as the authority exercised by an independent, self-governing entity over a specific territory and its population. The advent of digital technologies, alongside the rise of dominant technology companies upon which modern societies increasingly depend, has brought the issue of digital sovereignty to the forefront[11].

A) Sovereignty:

State sovereignty has historically rested on the premise that authority is exercised over a defined territory. For governments to maintain complete and exclusive control, events must be anchored to

specific locations, with jurisdiction demarcated by clearly delineated borders that officials can rigorously enforce[12].

1. The Scope of State Sovereignty:

However, a series of tangible developments have diminished the scope of state sovereignty. The modern state has become increasingly incapable of controlling new phenomena, such as evolving social relations shaped by globalization, which are not confined to limited territorial spaces where exclusive legal authority might be asserted. The proliferation of benefits and interactions untethered from geographical boundaries, coupled with the dissolution of these borders amidst the torrent of electronic and other forms of information, has eroded critical conditions for effective sovereignty[13].

2. Transition of The Concept:

The transmission of electronic data, the consequences of technological errors, and telecommunications cannot be restricted by conventional border checkpoints. Global media platforms now serve as arenas for state dominance at the level of users and educational trends. Alongside these material shifts, globalization has disrupted several established cultural and psychological foundations of sovereignty, particularly through the emergence of computer-linked communities formed around news and information on the World Wide Web. [14]

In this context, globalists predict the eventual dissolution of the territorial state as a sovereign entity defined by geographic boundaries, while the sovereign state itself strives to safeguard internal interests and act as a protective barrier against external threats. Increasingly, the focus of sovereign states has shifted toward global issues rather than national priorities.

Across nations, both citizens and leaders are increasingly convinced that the traditional geographical system of governance embodied by the state cannot adequately address transnational phenomena arising within the sphere of contemporary information and communications. The concept of sovereignty has thus transitioned from a political construct centred on geographic locations to a new model, crystallized through advancements in digital information technology—most notably the Internet and other digital media[15].

B) Digital Sovereignty:

To fully examine the notion of data sovereignty or digital sovereignty, it is important to recall the historical dominance and extensive control over discourse, particularly in Europe, across centuries marked by struggles between various power structures and ongoing political debates regarding sovereignty. The concept of sovereignty gradually took shape through the works of influential thinkers such as Jean Bodin, Grotius, Thomas Hobbes, John Locke, Montesquieu, and Rousseau, each of whom viewed sovereignty as the capacity to act independently, without external interference[16].

1. Classical Understand:

The classical understanding of sovereignty was especially shaped by the political theorists of the sixteenth century. Jean Bodin, for example, asserted that ultimate decision-making authority and the exclusive right to use force within the state should reside solely with the ruler—the sovereign. Later, in the eighteenth century, the Enlightenment philosopher Jean-Jacques Rousseau introduced a fundamental shift by transferring the concept of sovereignty from the hands of the ruler to the collective will of the people. As modern democracies evolved, Rousseau's perspective gained prominence, supporting the view that ultimate authority rests with the people, who may delegate this authority to a sovereign and democratically elected government[17].

The concept of sovereignty is also intrinsically linked to the territorially defined nation-state, wherein a state is regarded as sovereign if it can operate largely independently in its political, economic, and societal relations with other states. In the same context, sovereignty also implies the guarantee of citizens' capacity to exercise their inalienable rights. The intent is to empower all individuals to uphold and act upon their personal rights, anchored in their own authority. The responsibility to ensure the conditions for such autonomy falls to the state, especially considering the numerous challenges imposed by digital transformation on every sector of society. As a result, the term digital sovereignty has gained prevalence in contemporary discourse and encompasses a range of meanings, some of which are outlined below[18]:

The notion of "digital sovereignty" emerged at the beginning of the twenty-first century[19]. Notably, one of the earliest definitions appeared in 1983, articulated by Grant: "It is the ability and freedom to test, generate, acquire, build, or advance the technology necessary for industrial innovation." Grant's interpretation of digital sovereignty is structured around two key elements: the freedom to develop or utilize acquired technology—meaning the absence of contractual or legal restrictions—and "the ability to do so."

Pierre Bellanger, CEO of the French radio station Skyrock, made an early attempt to define digital sovereignty in 2011 as "the control of our present and our destiny guided by the use of technology and computer networks."[20]. A close examination of the principal debates shaping the relationship between sovereignty and digital networks, as well as the varied claims to digital sovereignty, reveals that sovereignty operates as a discursive practice in politics, rather than as a strictly legal or regulatory concept in the traditional sense. Digital sovereignty is now a shared objective among companies, public authorities, stakeholders, and, more recently, Internet users, citizens, and consumers.[21]

2. Other senses:

Accordingly, the term digital sovereignty is also used to describe society's autonomy in relation to technology, particularly its capacity to develop and utilize tools tailored by or for that society. This viewpoint serves as a primary avenue for cultural influence. Given the immense power wielded by technology companies, such as digital service providers like Facebook and Google, which deliver services based on their own cultural frameworks rather than those of their diverse user bases, states have found themselves increasingly unable to safeguard their citizens from the pervasive influences of the Internet. As a result, the onus now falls on states to construct and assert their own digital sovereignty[22].

Digital sovereignty, therefore, represents an inherently ambiguous concept, interpreted and utilized in diverse ways by various stakeholders. Despite this variability, the frequent invocations of digital sovereignty share several fundamental characteristics, though these are subject to differing interpretations depending on the actor involved. The concept has become increasingly urgent for states, as traditional mechanisms of sovereignty are now profoundly entangled with digital technologies, complicating the ability of states to assert effective control within their borders. The global, borderless nature of cyberspace enables malicious attacks on digital infrastructure, resulting in far-reaching economic and social consequences[23].

Additionally, as individuals become more interconnected through technological advancements, both governments and certain corporations have acquired enhanced surveillance capabilities, posing risks to personal freedoms and eroding individual sovereignty.

Digital sovereignty, in this sense, diverges from digital transformation, which refers to the widespread adoption of digital technologies across multiple sectors of society and the economy to improve efficiency and foster innovation. While digital transformation is vital for modernization, digital

sovereignty is primarily concerned with ensuring that technological advancements are managed under the auspices of state authority, safeguarding data privacy, cybersecurity, and digital rights.[24].

Digital sovereignty is often understood as the capacity to act autonomously in the digital realm, or to balance technological dependencies, through the implementation of protective mechanisms such as regulation and the deployment of proactive tools to encourage digital innovation, including the establishment of technological ecosystems and investment in innovation[25]. At its core, digital sovereignty demands control at three critical layers: the physical layer (resources, infrastructure, and devices), the code layer (standards, rules, and system design), and the information layer (content and data)[26].

Control in this context encompasses the ability to influence and restrict the manufacturing process (including the extraction and processing of raw materials), as well as the design, use, and outputs of digital technologies. Unlike interpretations that exclusively connect digital sovereignty to democratic legitimacy, this approach remains neutral regarding the normative criteria of such legitimacy[27].

Beyond the foundational aspect of control, different actors associate digital sovereignty with a variety of tools and strategies. States and supranational organizations may pursue digital sovereignty through capacity-building, investment, or regulatory measures[28].

Section III: Digital Sovereignty: Analytical Dimensions and Empirical Challenges.

This section extends beyond descriptive analysis to critically evaluate the practical operation of digital sovereignty, highlighting asymmetries of power among states, corporations, and users, and revealing the structural constraints confronting developing nations within the global digital order.

A) Actors in digital sovereignty:

The principal actors in the domain of digital sovereignty can be identified as follows:

1. **Cyber Justice:** This sphere is characterized by contention, with significant investments from numerous countries. It also serves as a battleground for technicians supporting extremist ideologies, terrorist networks, NGOs, and intelligence firms. The pursuit of divergent objectives enriches the landscape, with certain mutual interests occasionally intersecting. It is also the domain where vast quantities of big data are aggregated as users navigate the Internet, reflecting the sites visited and opinions expressed[29].

2. **ICT companies**: These entities strive to enhance their services and optimize advertising by collecting user data, exerting control over their production chains, managing the infrastructure essential for data transfer, and even dominating user interfaces (software) and connected devices. Their activities increasingly encompass services beyond their core specializations. For instance, Google offers email and mapping services in addition to its primary functions, all with the aim of maximizing profit.[30].

3. **Academic entities:** Institutions within the education sector play a pivotal role by preparing society for the digital future. They contribute to digital sovereignty over the long term by equipping citizens with the knowledge to understand both the risks and the potential for innovation, empowering them to become active participants within digital networks [31].

4. **The user:** The user is a dynamic and strategic agent within digital ecosystems. While digital spaces provide opportunities for self-expression and employment, they simultaneously pose threats to individual freedoms[32].

5. **Official actors:** Intelligence agencies, political authorities, and related entities function as major players by storing, analyzing, and monitoring information[33].

6. **Civil society:** Composed of independent, democratic, and voluntary institutions—including numerous non-governmental organizations such as human rights groups—civil society organizations act as key stakeholders in the digital sovereignty landscape.[34]

B) Dimensions of Digital Sovereignty:

1. **The power of agents:** Digital sovereignty encompasses the capacity of agents to wield power through the use of data, digital technologies, and associated infrastructures. This power is often challenging to exercise effectively, as the flow of information in the digital domain is not restricted by national boundaries. In this environment, traditional forms of sovereignty anchored in geospatial domains are disrupted, compelling nation-states to devise new mechanisms for exercising authority within cyberspace. These shifts are not isolated from the influence of earlier technological innovations—such as telegraphy, broadcasting, and satellites—each of which contributed to changes in the configuration and operation of political institutions and processes. For states to exercise digital sovereignty successfully, it is essential that they possess the capacity to assert control over relevant domains and processes. In such cases, they can at least regulate who is granted access, the purposes for which data may be used, who is authorized to process it, and most importantly, how access and processing impact the freedom of agents. It becomes clear, however, that digital sovereignty entails more than just the possession of absolute power within the digital sphere or its subdomains[35].
2. **Sovereignty as embodied power:** This dimension refers to the plurality of claims made by various embodied agents, extending beyond the state itself. It seeks to examine the ways in which sovereignty can be effectively exercised and maintained, and addresses how sovereignty transforms the very forms of life within which it is practiced. This raises important questions about which entities should be acknowledged as sovereign actors; sovereignty in this context can be exercised by individuals, organizations, or groups[36].
3. **Sovereignty as institutional power:** Digital sovereignty, in this sense, is neither autonomous nor self-sufficient, but is fundamentally dependent on the interplay between sovereignty and the relative differences for which sovereignty is claimed. This reliance on relative difference becomes evident in digital sovereignty through a range of normative claims made by one or more agents toward others. A significant consequence is the necessity for tangible spaces in which these claims can be articulated, negotiated, and renegotiated. Just like traditional sovereignty, digital sovereignty may be claimed, granted, recognized, and critiqued. Here, the central conceptual tension in digital sovereignty is found in the balance between sovereignty as a manifestation of control and as a basis for mutual recognition among actors[37].

C) Challenges of Digital Sovereignty:

1. **Economic and industrial challenges:**

Technological advancements in the digital sphere have generated new opportunities for synergy and collaboration, while simultaneously creating fresh avenues for competition, thus intensifying the complexity of global power dynamics. No society remains immune to scientific, economic, and commercial espionage, making the protection of companies and the confidentiality of data an urgent priority. Digital sovereignty serves as a crucial means to counteract the extraction and exploitation of data for commercial and marketing objectives[38].

2. **Political challenges:**

Economic and industrial policy concerns are also critical when asserting the desired level of digital sovereignty. Digital sovereignty functions as an instrument of governance and institutional protection, enabling the restoration of citizen trust, the defense of privacy and personal data, and the safeguarding of vital national infrastructure[39].

3. **Legal Challenges**:

A range of legal issues and questions arise that impact the capacity of states and institutions to preserve sovereignty and exert control over digital data and systems. Legislation pertaining to the protection of personal data and the assurance of privacy is central to advancing digital sovereignty, as such laws impose rigorous obligations on governments and institutions to secure the data of citizens and clients[40].

4. **National security issues:**

Major challenges have emerged for countries, corporations, and individuals alike, as evidenced by incidents such as the Cambridge Analytica scandal, which involved the manipulation of data to influence electoral outcomes. Other threats include hacking, data manipulation, sabotage, terrorism, identity theft, and bank card fraud, all of which have elevated computer security to the level of a national priority. The significance of digital sovereignty thus lies in its capacity to secure cyberspace for citizens, businesses, and states alike[41] .

5. **Strategic bets:**

A core strategic imperative is to prevent data leakage to foreign jurisdictions, particularly the United States of America. Preserving an independent capacity for decision-making and action is vital, as is safeguarding national sovereignty in the face of new threats arising from the accelerating digitalization of society[42].

6. **Security challenges:**

Security concerns associated with digital sovereignty have escalated rapidly, impacting regions worldwide. These threats encompass cyberattacks targeting critical infrastructure, acts of sabotage and physical assaults on network assets, disinformation campaigns, cyber espionage, and other malicious activities[43].

7. **Social challenges:**

On the societal front, the rapid spread of digital technologies has accelerated citizen empowerment by offering new opportunities, while simultaneously exposing individuals to novel forms of surveillance and repression.[44]

The pervasive diffusion of digital technologies and their impact on digital sovereignty intersect with a broad spectrum of issues—democratic, economic, social, commercial, industrial, defense, and security concerns. Beyond economic factors, the very fabric of social models and their underpinning values is at stake. When viewed collectively, these domains challenge the integrity and independence of state jurisdiction, ultimately representing a fundamental and existential question: the ability of states to maintain control over their essential jurisdictions and to apply the values that shape their identity and organize social relations..[45]

D) Policies and coping mechanisms :

Nations are adopting comprehensive, multi-layered policies and strategies across various domains to establish and reinforce digital sovereignty. These approaches include sustainable plans designed to

enhance control over digital technologies, data, and national information, functioning as the first line of defense against emerging threats. Such strategies are the foundation for raising awareness, improving digital efficiency, and safeguarding national sovereignty in cyberspace, and may be categorized as national or international policies.

A. **Local-Level Coping Policies:**

Local responses encompass a suite of internal measures aimed at developing digital infrastructure, regulating technology, updating legislation, securing data, monitoring networks and communications, and promoting digital citizenship.

1. **Developing Digital Infrastructure:** Investment in robust digital infrastructure is essential. This includes establishing high-speed, reliable communication networks, ensuring widespread access to information, bolstering network security, and implementing local cloud storage solutions. Such development enhances the capacity to effectively track data and provide secure, dependable digital services for citizens. Sustainability depends on effective management and the integration of three critical dimensions: technological, physical, and cultural infrastructure.
2. **Localization of Technology:** This process begins by fostering a knowledge system that is adaptable and accessible, overcoming material and intellectual barriers to facilitate knowledge acquisition. It involves efforts to transfer and produce technology domestically, ultimately achieving technological mastery—a state of self-sufficiency and competitive capability. This stage, marked by the emergence of qualified national expertise in technology production and industry, enables a country to keep pace with rapid change and continually adapt, an approach known as "strategic flexibility."
3. **Developing Legislation and Policies to Protect Personal Data:** Enacting rigorous legislation to safeguard the personal data of citizens and residents is paramount. This entails developing policies to govern the volume, use, sharing, and storage of data, ensuring alignment with stringent privacy and security standards.
4. **Monitoring and Controlling Networks and Communications:** States must build capacities to monitor and manage digital networks and communications, enabling prompt identification and mitigation of cyber threats. This includes deploying advanced intrusion detection technologies and conducting regular surveillance to counteract illicit activities.
5. **Promoting Digital Citizenship:** Promoting digital citizenship involves raising awareness about internet risks, fostering ethical and responsible online conduct, respecting others' rights, encouraging active engagement—including digital political participation—and offering targeted training. Policies should be implemented to enhance transparency and accountability in digital technology use and data collection. Mechanisms must be established for the oversight of digital technology utilization by both governmental and private entities, all while protecting citizens' rights and upholding national sovereignty.

B. **Policies at the international level :**

1. **Digital Cooperation:** International collaboration among digital partners—such as those within the United Nations—enables the collective addressing of digital challenges at the global level. The announcement of the Digital Charter and its global adoption, commemorating the 70th anniversary of the United Nations in September 2020 and scheduled for formal approval at the September 2024 Summit, exemplifies this commitment. This charter encompasses all sectors: contemporary businesses, the UN system, the private sector (including major technology companies), civil society,

grassroots organizations, academia, and individual actors, including youth. Notably, the Global Digital Charter seeks to "identify common alternatives for a digitally open and secure future for all." The proposed agenda covers digital communications, Internet governance, the right of individuals to control the use of their data, the protection of human rights online, and the preservation of Internet reliability through harmonized accountability standards to prevent misleading practices.

2. **Governance of digitalization :** Digitalization of public services offers opportunities to enhance governance outcomes by increasing transparency, auditability, and oversight. Extensive evidence supports the notion that these factors improve governance outcomes. Research indicates that strengthening accountability, open access to government data, and robust public administration can positively influence the delivery and quality of healthcare and other public services[46].

Digital governance is designed to ensure that digital technologies contribute to outcomes that are inclusive, secure, and equitable. Effective governance is essential for harnessing the developmental benefits of digital technologies and for mitigating associated risks. Nevertheless, the digitization of government services introduces new risks, including heightened surveillance and the amplification of discrimination. Emerging technologies, such as artificial intelligence and advanced biometrics, present additional challenges—such as mass surveillance, algorithmic bias, and opacity in decision-making processes—which may result in unfair outcomes, violations of privacy, and misuse of data. Automated decision-making systems, powered by AI, carry particular risks in terms of amplifying societal biases and limiting avenues for redress, as these systems are typically trained on large datasets that may encode existing prejudices.

Digital governance is a responsibility shared by the global community, sovereign states, citizens, and a range of non-traditional actors. However, evidence demonstrates that governance disparities exacerbate existing gaps. The Algerian case serves as a salient example of the structural challenges faced by developing countries striving to assert digital sovereignty within a global digital order characterized by asymmetries. Despite heightened awareness of the strategic importance of data protection, cybersecurity, and digital infrastructure, Algeria remains constrained by technological dependence, limited domestic production of digital technologies, and continued reliance on foreign platforms and cloud services. These dependencies undermine the state's capacity to control data flows and safeguard critical digital infrastructure, thereby limiting the full realization of sovereignty in cyberspace.

Nonetheless, Algeria has initiated efforts to reinforce its digital sovereignty through the development of regulatory frameworks, implementation of data protection policies, and advancement of cybersecurity strategies. These measures—emphasizing the protection of national data, oversight of digital communications, and modernization of public administration—reflect attempts to reassert state authority within the digital domain. However, such initiatives are primarily defensive and regulatory in nature rather than productive and innovative, as the lack of a robust national digital ecosystem and restricted investment in advanced technologies hinder Algeria's strategic autonomy.

From a geopolitical perspective, the Algerian experience reflects a broader trend observed in many Global South countries, where digital sovereignty is pursued predominantly through regulation and control, rather than through technological innovation and leadership. This dynamic perpetuates global hierarchies, with technological power concentrated in a limited number of dominant states and multinational corporations. Accordingly, digital sovereignty in Algeria is best understood not as an achievement of absolute autonomy, but as a contested and evolving process shaped by global technological dependencies, regional power structures, and domestic challenges in capacity-building.

The European Union, by contrast, offers a clear illustration of how digital sovereignty can be exercised through regulatory mechanisms rather than technological supremacy. Instruments such as the General Data Protection Regulation (GDPR) and the Digital Services Act exemplify how normative influence may be leveraged to compensate for technological dependence, revealing both the strengths and inherent limitations of regulatory sovereignty in the digital era.

Conclusion:

The study finds that sovereignty is undergoing a profound transformation in the digital age, no longer confined to geographic borders and physical control, but now encompassing cyberspace, data, and technology. Digital transformation has redefined international relations, elevating digital sovereignty as a fundamental component of national sovereignty. Emerging issues—such as cybersecurity, technological dominance, and the governance of cyberspace—have become decisive factors impacting the stability of the international system.

Among the principal findings:

- Digital transformation has introduced significant challenges for nations, particularly in safeguarding sovereign data and combating cybercrime.
- Technologically advanced, hegemonic states exert greater control over cyberspace, thereby deepening the technological divide between developed and developing countries.
- Digital sovereignty is not merely a continuation of traditional sovereignty, but a distinct concept that calls for a reassessment of international relations and the development of innovative policy frameworks.
- Technology has become a primary instrument of power and control within the global system, positioning it at the heart of contemporary geopolitical competition.

Ultimately, digital sovereignty must be regarded as a dynamic and contested form of power, rather than a static legal status. Its trajectory will depend on the capacity of states to reconcile technological progress with democratic legitimacy, international collaboration, and the safeguarding of individual rights in an increasingly fragmented digital landscape.

Recommendations:

- Enhancing Digital Sovereignty: States should develop comprehensive national policies to safeguard data and citizens from cyber threats, enacting stringent legislation to govern digital domains.
- International Cooperation: Cross-border collaboration must be strengthened to counter cybercrime and to establish universally accepted frameworks for cyberspace governance.
- Bridging the Technology Gap: Developing countries should prioritize investment in technological infrastructure and digital skill-building to mitigate dependency on more technologically advanced nations.
- Balancing Privacy and Control: There is a critical need to harmonize the protection of individual privacy with the exercise of state control in digital environments, in compliance with international legal standards.
- Forward-Looking Strategies: States and international organizations should implement long-term strategies to address the evolving impact of digital transformation on sovereignty, with an emphasis on digital ethics and robust security.

In conclusion, the digital era presents a significant opportunity to reconceptualize sovereignty in alignment with the demands of modernity. Realizing this potential requires that countries embrace adaptable and holistic policy responses that effectively balance the challenges of digital transformation with their core national interests.

Bibliography:

A- Books:

- Daniel Philpott: **Revolutions in Sovereignty** , USA: Princeton University Press, 2001
- Farid Gueham, "**Digital Sovereignty, Steps Towards a New System of Internet Governance**", France: The Fondation pour l'innovation politique, 2017.
- Giorgio Monti, "**Eu Competition Law And Digital Sovereignty**" In: Digital Sovereignty: From Narrative To Policy? Edited By Dennis Broeders, Raluca Csernatoni, Kristina Irion, Monica Kaminska, Giorgio Monti, Margarita Robles-Carrillo, Simona Soare, And Paul Timmers, Eu Institute For Security Studies, 2022.
- Hannes Werthner , "**Digital Transformation, Digital Humanism: What Needs to Be Done** ", in: Introduction to Digital Humanism, edited by: Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem and Allison Stanger, Switzerland: Stringer, 2024.
- Paul Timmers, "**Sovereignty in the Digital Age**" in: Introduction to Digital Humanism, edited by: Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem and Allison Stanger, Switzerland: Stringer, 2024.

B – Articles:

- .Jonathan Fried , "**Dimensions of Sovereignty--A Canadian Approach The**", Canada United State Law Journal, Vol. 24(7), 1998, PP. 17-26.
- Damiano Canale, "**Walled Borders, Territoriality and Sovereignty: A Tipology** ", Athena, Vol. 1(1), 2021, pp.37-57.
- Dilmurad Iakhiaev, Aleksei Grigorishchin, Lyudmila Voronina, Diana Dementeva, Irina Ivanova, "**Conceptual foundations and global challenges in the formation of digital sovereignty of the state**", Vol. 36(5), 2023, pp. 169-179.
- Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek, Timo Seidl, "**Digital sovereignty Rhetoric and reality**", Journal of European Public Policy Vol. 31, 2024, PP. 2099-2120.
- Huw Roberts Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, "Safeguarding European values with digital sovereignty: an analysis of statements and policies", Internet Policy Review 10(3) | 2021, Pp. 3-24.
- Huw Roberts, "**Digital sovereignty and artificial intelligence: a normative approach "**, Ethics and Information Technology , 26 (70), 2024, PP.1-10.
- John Agnew, "**Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics",** Annals of the Association of American Geographers Volume 95, 2005 - Issue 2, Pp. 437-461
- Julia Pohle & Thorsten Thiel," **Digital sovereignt**", Internet Policy Review, 9(4), 2020, PP.2-19.
- Matthias Braun and Patrik Hummel, "**Is Digital Sovereignty Normatively Desirable**", Information, Communication & Society, April 2024, PP.1-14.
- Milton Mueller, Georgia Institute of Technology, USA Digital sovereignty: What does it mean?, p.1.
- Ramona Gabriela Tătar And Adela MoișI, "**The Concept of Sovereignty**", Journal of Public Administration, Finance and Law, 24, 2022, PP. 292-303.

- Stephane Couture & Sophie Toupin McGill, " **What does the notion of "sovereignty" mean when referring to the digita**l?", new media & society , pp. 1–18.

C –Reports:

- Emrys Schoemaker, " Digital Technology and Governance: The role of governance in ensuring digital technologies contribute to development and mitigate" , USA: UNDP, 2024.
- Ines Mergel, "**Study on the impact of digital transformation on democracy and good governance**", Adopted by the CDDG following its 13th meeting, Strasbourg (15-16 April 2021).
- Melody Musoni, Poorva Karkare, Chloe Teevan and Ennatu Domingo, "**Global approaches to digital sovereignty: Competing definitions and contrasting policy**", The centre for Africa-Europe relations, May 2023.
- Resilience Julien, Nocetti Coordinator, Amar Rouabhi, Sara Baazobandi, Chloé Berger, "**Digital Sovereignty In The Mena Region: Overcoming Paradoxes To Ensure Digital**", IE med, euromesco Policy Study n:36, August 2024.
- Tambiama Madiega, "**EU Digital sovereignty for Europe**", EPRS Ideas Paper Towards a more resilient, July 2020.

D - Websites:

- NETmundial+10 – Global challenges for the governance of the digital world, on: https://netmundial.br/

Citations:

[1] Stephane Couture & Sophie Toupin McGill, " **What does the notion of "sovereignty" mean when referring to the digital?**", new media & society,P.3.

[2] Milton Mueller, Georgia Institute of Technology," **USA Digital sovereignty: What does it mean?**", p.1.

[3] John Agnew, "**Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics",** Annals of the Association of American Geographers 95, 2005, P. 441.

[4] Daniel Philpott, **Revolutions in Sovereignty** , USA: Princeton University Press, 2001, P. 7.

[5] John Agnew, "**Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics",** Op.cit, P.481.

[6] Stephane Couture & Sophie Toupin McGill, "**What does the notion of "sovereignty" mean when referring to the digital?"**, Op.cit, P.2.

[7] Ibid.

[8] Huw Roberts Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, "**Safeguarding European values with digital sovereignty: an analysis of statements and policies**", Internet Policy Review 10(3), 2021, P.5.

[9] Damiano Canale, "**Walled Borders, Territoriality and Sovereignty: A Tipology** ", Athena, Vol. 1(1), 2021, P.38.

[10] Jonathan Fried , "**Dimensions of Sovereignty--A Canadian Approach The**", Canada United State Law Journal, Vol. 24(7), 1998, P. 18.

[11] Ramona Gabriela Tătar And Adela MoișI, "**The Concept of Sovereignty**", Journal of Public Administration, Finance and Law, 24, 2022, P. 294.

[12] Pohle, Julia; Thiel, Thorsten, "**Digital Sovereignty**", In: Herlo, Bianca Irrgang, Daniel Joost, Gesche Unteidig, Andreas (Ed.): Practicing Sovereignty: Digital Involvement in Times of Crises, P. 48.

[13] Ibid, P.50.

[14] Melody Musoni, Poorva Karkare, Chloe Teevan and Ennatu Domingo, "**Global approaches to digital sovereignty: Competing definitions and contrasting policy**", The centre for Africa-Europe relations, May 2023, P.5.

[15] Ramona Gabriela TĂTAR and Adela MOIȘI, "**The Concept Of Sovereignty**", Op.cit, P. 295.

[16] Melody Musoni, Poorva Karkare, Chloe Teevan and Ennatu Domingo, "**Global approaches to digital sovereignty: Competing definitions and contrasting policy**", Op.cit, P.5.

[17] Ibid, P.5.

[18] Ibid, P.6.

[19] Farid Gueham, "**Digital Sovereignty, Steps Towards a New System of Internet Governance**", France: The Fondation pour l'innovation politique, 2017, P. 11.

[20] Ibid, P.11.

[21] Tambiama Madiega, "**EU Digital sovereignty for Europe**", EPRS Ideas Paper Towards a more resilient, July 2020, P.2.

[22] Dilmurad Iakhiaev, Aleksei Grigorishchin, Lyudmila Voronina, Diana Dementeva, Irina Ivanova, "**Conceptual foundations and global challenges in the formation of digital sovereignty of the state**", Vol. 36(5), 2023, P.173.

[23] Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek, Timo Seidl, "**Digital sovereignty Rhetoric and reality**", Journal of European Public Policy Vol. 31, 2024, P. 2103.

[24] Farid Gueham, "**Digital Sovereignty, Steps Towards A New System Of Internet Governance**", France: The Fondation pour l'innovation politique, 2017, P. 11.

[25] Ibid, P.12.

[26] Ibid, P.13.

[27] Julia Pohle & Thorsten Thiel," **Digital sovereignt**", Internet Policy Review, 9(4), 2020, P.3.

[28] Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek, Timo Seidl, "**Digital sovereignty - Rhetoric and reality**", Op.cit, P.2103.

[29] Paul Timmers , "**Sovereignty in the Digital Age**" in: Introduction to Digital Humanism, edited by: Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem and Allison Stanger, Switzerland: Stringer, 2024, P.574.

[30] Huw Roberts, "**Digital sovereignty and artificial intelligence: a normative approach "**, Ethics and Information Technology , 26 (70), 2024, P. 3.

[31] Paul Timmers , "**Sovereignty in the Digital Age**", Op.cit, P.575.

[32] Ibid.

[33] Huw Roberts, "**Digital sovereignty and artificial intelligence: a normative approach "**, Opc.it, P.4.

[34] Ibid.

[35] Matthias Braun and Patrik Hummel, "**Is Digital Sovereignty Normatively Desirable**", Information, Communication & Society, April 2024, P.6.

[36] Ibid, P. 7.

[37] Ibid, P.8.

[38] Julia Pohle & Thorsten Thiel," **Digital sovereignt**", Op.cit, P.50.
[39] Ibid, P.51.
[40] Giorgio Monti, "**Eu Competition Law And Digital Sovereignty**" In: Digital Sovereignty: From Narrative To Policy? Edited By Dennis Broeders, Raluca Csernatoni, Kristina Irion, Monica Kaminska, Giorgio Monti, Margarita Robles-Carrillo, Simona Soare, And Paul Timmers, Eu Institute For Security Studies, 2022, P. 46.
[41] Resilience Julien, Nocetti Coordinator, Amar Rouabhi, Sara Baazobandi, Chloé Berger, "**Digital Sovereignty In The Mena Region: Overcoming Paradoxes To Ensure Digital**", IE med, euromesco Policy Study n:36, August 2024, P.25.
[42] Ibid, P.26.
[43] NETmundial+10 – Global challenges for the governance of the digital world, on: https://netmundial.br/
[44] Ibid.
[45] Resilience Julien Nocetti Coordinator Amar Rouabhi Sara Baazobandi Chloé Berger, "**Digital Sovereignty In The Mena Region: Overcoming Paradoxes To Ensure Digita**l", Op.cit, P.26.
[46] Emrys Schoemaker, " **Digital Technology and Governance: The role of governance in ensuring digital technologies contribute to development and mitigate**" , USA: UNDP, 2024, P.7.