



Digital Sovereignty in Algeria: A Legal and Institutional Analysis of Digital Transformation and Cybersecurity

La souveraineté numérique en Algérie : une analyse juridique et institutionnelle de la transformation numérique et de la cybersécurité

Dr. Guenad Mohammed*¹,

Faculty of Law and Political Sciences, University of Tlemcen, Algeria, Email:

mohammed.guenad@univ-tlemcen.dz

Dr. Mahcer Lotfi²,

Faculty of Law and Political Sciences, University of Tlemcen, Algeria, Email:

lotfi.mahcer@univ-tlemcen.dz

Received: 01/06/2026

Accepted: 25/09/2026

Published: 30/09/2026

Abstract :

The wave of change in communication and information has driven all governments to shift toward electronic administration. The deep qualitative and quantitative transformations of the digital age—alongside a digital revolution affecting all aspects of life—have notably impacted state sovereignty. Furthermore, digital threats that transcend the traditional concept of sovereignty have created a new form of digital vulnerability. Consequently, the continuity of nations today relies heavily on their ability to protect their digital sovereignty from cybersecurity threats, requiring a robust cyberdefense strategy that establishes a comprehensive defense system encompassing both technical and legal aspects.

This study examines the importance of digital transformation in Algeria, measuring its impact on addressing societal challenges on one hand and activating sustainable development on the other. In this regard, we seek to evaluate the extent to which digital transformation contributes to serving the public interest by analyzing the underlying motives for adopting digitization through the electronic administration mechanism.

Keywords: Digital Sovereignty, Digital Transformation, Public Service, E-Government.

Résumé:

La vague de changement dans la communication et l'information a poussé tous les gouvernements à s'orienter vers l'administration électronique. Les transformations qualitatives et quantitatives profondes de l'ère numérique — ainsi qu'une révolution numérique touchant tous les aspects de la vie — ont sensiblement affecté la souveraineté de l'État. De plus, les menaces numériques qui transcendent le concept traditionnel de souveraineté ont créé une nouvelle forme de vulnérabilité numérique. Par conséquent, la continuité des nations dépend aujourd'hui fortement de leur capacité à protéger leur souveraineté numérique face aux menaces de cybersécurité, ce qui nécessite une stratégie de cyberdéfense robuste établissant un système de défense global englobant à la fois les aspects techniques et juridiques.

Cette étude examine l'importance de la transformation numérique en Algérie, en mesurant son impact sur la résolution des défis sociétaux d'une part, et sur l'activation du développement durable d'autre part. À cet égard, nous cherchons à évaluer dans quelle mesure la transformation numérique contribue à servir l'intérêt général en analysant les motifs sous-jacents de l'adoption de la numérisation à travers le mécanisme de l'administration électronique.

Mots-clés : Souveraineté numérique, Transformation numérique, Service public, Gouvernement électronique.

Introduction:

The wave of change in the field of information delivery and communication has pushed all governments towards electronic management. Therefore, we find several developments driving the adoption of electronic management, including those related to government officials who are developing new methods to improve government work. This is to increase the efficiency of service delivery and sometimes in response to pressures from citizens, the business sector, or other parties related to government work and we find that in every country, there are real motivations that call for the transition to electronic governance considering other motivations. Depending on the economic and political situation of this country, the most important of these motivations are as follows.¹

- The acceleration of scientific progress and technological development: With the spread of electronic culture and the advancement of communications, which have led to the interconnectedness of human societies through globalization trends towards a global village.

- The shift from traditional management styles to the new management thinking based on communication and information technology, understanding it from an administrative perspective that focuses on defining the organization's strategic goals and exploring

The appropriate technologies capable of helping it achieve its goals.

- There are many reasons that have prompted many countries and organizations to hasten the implementation of e-governance in their management, including:

- The internet as a global network has made the world a small and homogeneous village.

- Globalization, which has been considered a driving force for many countries to improve their services and rise to global standards.

To obtain the global quality certification for its service in terms of citizen satisfaction on the other hand.

- The trend towards privatization has increased, as this trend has pushed the new world of countries towards privatizing their services.

- In addition to administrative procedures and complex operations and their impact on increasing business costs.

- The difficulty of providing circulating data to employees in the organization

- The necessity of achieving continuous communication among employees as the scope of work expands it becomes clear to us that the primary reason for accepting the idea of electronic management, which is an alternative to traditional management, is the necessity to respond to

¹ Yves Guichet, Constitutional Law; Ellipses, Paris, 1996.



the requirements of both internal and external environments. The internal environment generates a lot of information and employee and worker records, which are difficult to control. Externally, due to numerous transactions with partners, suppliers, and others, there is an excess of information about them and a lack of control. Electronic management relies on computers in its various transactions, which contributes to controlling these aspects based on the above, we pose the following question:

To what extent does the internet affect state sovereignty?

1- Concept of Digital Sovereignty

1-1 The Concept of Classical Sovereignty

It seems there is no text to translate. Please provide the text you'd like me to translate. Sovereignty is the fundamental legal characteristic of the state. While the state shares with other entities the acquisition of legal personality, it alone possesses sovereignty. Meaning that it has the supreme authority that no other power or body can surpass, and this makes it superior to all others, considering itself as the supreme commanding authority². Therefore, state sovereignty simply means that it is the source of other authorities. Sovereignty is original and inherent to the state, distinguishing it from other political entities. Sovereignty is a single, indivisible unit, regardless of the number of public authorities, as these authorities do not share sovereignty but rather share jurisdiction.³

Sovereignty is original and inherent to the state, distinguishing it from other political groups. Sovereignty is a single unit that cannot be divided, no matter how many public authorities there are, because these authorities do not share sovereignty but rather share jurisdiction. The term "sovereignty" is derived from the Latin word "supraners," meaning "the highest." This concept was developed by the jurist Jean Bodin in his six books on the Republic in 1576. The word "sovereignty" is derived from the Latin word "supraners," meaning "the highest." This concept was developed by the jurist Jean Bodin in his six books on the Republic in 1576.

The term "sovereignty" is derived from the Latin word "supraners," meaning "the highest." This concept was developed by the jurist Jean Bodin in his six books on the republic in 1576. Thus, the sovereign nature of state authority means its independence and lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities without dispute. It also allows the state to exclusively organize the fundamental affairs of society, whether related to private or public relations, through the institutions created for this purpose. So, the meaning of the sovereign nature of state authority is its independence and lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities without dispute. It also allows it to take sole responsibility for organizing the fundamental affairs of society, whether related to private or public relations, through the institutions established for this purpose.⁴

² _

³ Dominique Rousseau "the constitution or politics differently" *Débat* magazine, no. 64, March 1991, p. 183

⁴ Favoreu Louis "Constitutional Law: Law of the Constitution and Constitution of the Law," *French Review of Constitutional Law*, no. 1, 1990, p. 79



So, the concept of the sovereign authority of the state refers to its independence and its lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities without dispute. It also allows the state to take sole responsibility for organizing the fundamental matters of society, whether they pertain to private or public relations, through the institutions established for this purpose. Consequently, sovereignty entails a set of consequences. Consequently, sovereignty entails a set of outcomes, which are:

- The state is the only institution that holds an inherent authority not derived from any other authority that precedes or follows it.
- This sovereignty, represented by that authority, is a supreme sovereignty that is not surpassed by any other authority, neither within the state nor outside it.
- The state, as the owner of that sovereignty, is the one that determines and establishes its legal organization throughout its national territory, which includes moral principles and material rules, without being influenced by factors other than the requirements of national sovereignty.
- The state is the starting point and source of all authorities that arise from that political and legal organization.
- The state uniquely determines its competencies and the scope of its influence.
- The state, as a result of the above, monopolizes the manifestations of sovereignty that it exclusively holds, such as the public force including the army and police, the minting of currency, and so on.

The state, as a result of the above, monopolizes the manifestations of sovereignty, such as the public force, the army, the police, the issuance of currency, and so on. Based on these results, it can be said that the state's enjoyment of sovereignty makes its authority original, supreme, unified, and indivisible. Based on those results, it can be said that the state's enjoyment of sovereignty makes its authority an original, supreme, and indivisible one.

1- Forms and manifestations of sovereignty: Sovereignty is divided into legal and political forms, and it is practically manifested through various fields or aspects, both internally and externally, as well as regionally and personally.

A- Forms of sovereignty: The authority of the state is characterized by being legal and political sovereignty. Legal sovereignty refers to the state's authority to issue legislation through its representatives, enforce it, and punish anyone who violates it. As for political sovereignty, it refers to the people in its political sense, who are credited with choosing the political officials who have the right to exercise legal sovereignty. Thus, it is the authority of the people to choose those who will be responsible for managing public affairs in the state.

B- Aspects of Sovereignty: Sovereignty has several fields or aspects, the most important of which are:

- Internal sovereignty and external sovereignty: Internal sovereignty refers to the supreme authority of the state exercised over individuals and entities within its territory. Accordingly, it can issue orders, legal rules, and general directives that have binding force and must be obeyed by individuals. It is also capable of performing all actions of particular importance to governance and politics, such as drafting the constitution, determining the system of government, imposing taxes, maintaining order, managing public facilities, minting currency,

directly supervising the judiciary, monopolizing internal and external defense tasks, and undertaking the mission of maintaining security and public order... All these actions express sovereignty in its positive sense. The state is subject only to its independent and singular will, due to the supremacy and elevation of its authority and the absence of any higher or parallel authority as for external sovereignty, it is the sovereignty exercised by the state in relation to other states, meaning the set of rights and powers it exercises in the international community, in its foreign relations, such as the right to conclude treaties and international agreements, the right to diplomatic representation and joining international organizations, the right to declare or end war, as well as the right to follow up on and protect the affairs of its nationals abroad. Thus, sovereignty in this sense is of a negative nature because it does not impose specific actions on the state except for the restrictions imposed by international law and the treaties and agreements it has freely entered into.

However, a state's external sovereignty can be complete or incomplete. It is complete if the state is fully independent and not subject to another state, which is referred to as fully sovereign states. External sovereignty is considered incomplete if the state retains some aspects of its external sovereignty while losing others, due to its subordination to another state, such as protectorates and territories under mandate or trusteeship, which are referred to as partially sovereign states.

- Territorial sovereignty and personal sovereignty: Territorial sovereignty defines the state's exercise of its sovereignty within the boundaries of its territory, where it practices all aspects of sovereignty, including the authority to command and prohibit, impose penalties, and issue laws and regulations to be applied to everyone within its territory, regardless of their affiliation with its people. Therefore, territorial sovereignty is determined by the presence of individuals within its territory, whether they are citizens or foreigners, and as a result, the state has no authority over its citizens if they are outside its territory.

As for personal sovereignty, it is where the state defines the scope of its sovereignty over the individuals who make up its people and enjoy its nationality, whom it calls "citizens or subjects" and who hold its nationality. The state exercises personal sovereignty over its citizens, whether they are within the state's territory or outside it in the territory of a foreign state. Accordingly, under this sovereignty, the state has the right to track its citizens in foreign countries, but it does not exercise this sovereignty over foreigners residing within its territory because they are not its citizens.

Digital sovereignty is considered one of the modern concepts in management science, resulting from many developments that contemporary societies have experienced since the transition to electronic work to improve public service and reduce material expenses by introducing modern technologies and means, including information systems. The system is defined in two ways: one is a concise definition, such as the following: a system is a set of elements that integrate with each other to achieve a specific goal. The expanded definition describes it as a set of interrelated components that work together to achieve a common goal. Inputs are accepted for systematic processes to produce outputs.

The definition of information is data that has the quality of credibility and is presented for a

specific purpose or goal. Information is developed and elevated to the status of knowledge when used for comparison and evaluation of previous and specific results and for the purpose of communication. As for the information system, it is defined as a systematic way to store data and information about each user with the aim of assisting in planning, decision-making, and providing complete reports on every activity that serves the organization's goals.

Lucas defined it as a set of procedures, software, machines, installations, and methodologies necessary for data processing and retrieval, which are essential for managing the organization's activities as for the Human Resource Information System, it is defined as a system designed to perform a specific function within the organization's operations, specifically to manage human resources and primarily to provide the information needed by managers to make decisions related to the effectiveness and efficiency of human resource utilization, enhancing performance levels to fulfill their role in achieving organizational goals.

1-2 The concept of digital sovereignty

The concept of digital sovereignty and the changes occurring in the global system, along with new transformations in concepts and roles, have led to the emergence of new actors who now share the sovereignty of states. This is achieved through the creation of what is called soft power, which works to change concepts towards reality by overwhelming the system with a massive amount of information, making the ability to absorb it minimal. Therefore, one of the most significant challenges we face today in decision-making and achieving developmental goals is the ability to discern the truthfulness of information among the topics related to the concept of "digital sovereignty" and "requirements for societal security and digital development," the lecture aims to "enable various national institutions to benefit from studies conducted by several Algerian professors in the fields of cyber warfare and awareness plans, and to address various terms and meanings⁵, as stated by the organizers of the scientific event." It will work on this sensitive issue, which is experiencing significant developments and qualitative leaps in its aspects related to wars, influence, and espionage, with the aim of forming a scientific culture on how to use virtual domains and maintain vigilance against any attempts to breach or attack the institutions and resources of the nation.

This topic: "Based on regional and global contexts witnessing widespread dissemination of modern technologies, virtual spaces, and artificial intelligence, and their use to provoke crises and as a weapon."

And in the context of supporting the efforts of the state and various institutions to instill a cyber culture that contributes to enhancing Algerian national security.

Countries, economies, and societies have come under the threat of digital attacks. Sovereignty has taken on a digital face.

So, what does digital sovereignty mean? What are its pillars? What is its relationship with political and economic national sovereignty, and the security and stability of societies? And what is its position in the international competition for influence?

⁵ -Pauline Türk, "Définition et enjeux de la souveraineté numérique," *Les Cahiers français*, no. 415 (May-June 2020), 18.

And technology has begun to be used to influence sovereignty, so the borders of virtual countries must be protected from internal concepts, especially those related to social media that need to be regulated because they represent fertile ground for promoting electronic campaigns that attempt to undermine the sovereignty of countries and manipulate and destabilize public opinion digital sovereignty is "the ability of countries to operate in the electronic space and ensure that their rules are respected by various actors in the virtual world."⁶

The virtual space and its interactions, along with modern technologies, are intensively used in wars and conflicts. The latest example was in Lebanon when the Zionist entity detonated communication devices in the hands of their owners, resulting in the deaths of many of them, in addition to exploiting the virtual space in psychological warfare.

The threat to sovereignty no longer comes only from massive armies and deadly weapons. It can also come from digital devices and programs that only need to manipulate symbols, numbers, and secret channels.

The concept of digital sovereignty is "linked to the sensitivity of data and electronic information and the importance of preserving them," and that "many countries face significant challenges in securing their cyberspace amid digital transformations."

Current threats "are not limited to military wars, but have extended to digital and software technologies that require adopting new strategies and approaches⁷."

Cyber threats are considered a new face of colonialism and their impact on the sovereignty of nations, calling for the adoption of defense strategies based on developing infrastructure and investing in local human resources⁸.

Algeria fully recognizes the importance of digital sovereignty and strives to enhance it through the national digital transformation strategy outlined by the President of the Republic, Mr. Abdelmadjid Tebboune, in order to build an inclusive digital economy, improve public services, and promote digital integration within the framework of protecting and securing personal data.

2 The Status of Digital Sovereignty in Algerian Legislation

He clarified in this regard that the Algerian legislator "established state control over its digital space as a confirmation of its sovereignty and an enhancement of the guarantee of the privacy and sanctity of its citizens and anyone present on its territory," referring to Law 07-18 related to the protection of natural persons in the field of processing personal data, which is considered "a constitutional mechanism for establishing the legal framework for the data processing system in our country, and addressing the repercussions of the rapid development of information and communication technologies on private life, personal freedom, honor, and reputation⁹."

And also Law No. 12-12 dated 14 Sha'ban 1430, corresponding to August 5, 2009, which includes specific rules for preventing and combating crimes related to information and communication technologies.

⁶ -*Souveraineté numérique*, Assemblée nationale, France, 2009.

⁷ -Solange Ghernaouti, "Comment lutter contre la cybercriminalité," *Pour la Science*, no. 391 (May 2010): 24–27.

⁸ -Olivier Kempf, *Introduction à la cyberstratégie*, 2nd ed. (Paris: Economica, 2015).

⁹ -Pauline Türk, "L'autodétermination informationnelle : un droit fondamental émergent ?," *Dalloz IP/IT*, no. 11 (November 2020): 616–620.

In this regard, he emphasized that the President of the Republic has given "special attention to protecting natural persons in the field of personal data processing" through "mechanisms for promoting and developing human rights and adapting care methods to technological advancements."

He mentioned that Algeria has worked on "keeping pace with technological advancements in media and communication by amending and enacting legislative texts that contribute to strengthening digital sovereignty, including the Electronic Communications Law, the Personal Data Protection Law, and the Cybercrime Law."

1-1 Law and Digital Sovereignty

Algerian legislation has addressed cybercrimes by issuing general and specific laws. The Algerian Constitution of 2016 also guaranteed the protection of fundamental rights and individual freedoms. These constitutional principles have been enshrined in practice through legislative texts included in the Penal Code and the Code of Criminal Procedure that prohibit any violation of these rights.

The Algerian legislator addressed the criminalization of acts affecting computer systems, amending the Penal Code by Law No. 04-10 dated November 10, 2004, which modifies and supplements Ordinance No. 66-106 containing the Penal Code, under the title: "affecting automated data processing systems."

This section includes eight articles from Article 394 bis to Article 394 bis 7.

In this law, the local jurisdiction of the Public Prosecutor in the field of cybercrimes has been extended, according to Article 37, Paragraph 2 of the Code of Criminal Procedure (Order 15-02, 2015). Local jurisdiction extends if it concerns drug offenses, organized crime crossing national borders, crimes affecting automated data processing systems, money laundering, terrorism, crimes related to foreign exchange legislation, corruption, and smuggling (Ohaibia, 2018, p. 358). The law also stipulates searches in Article 45, Paragraph 2 of the same amended law. Additionally, Article 65 bis 3, Paragraph 5 states that in cases of crimes affecting automated data processing systems, the competent Public Prosecutor can make technical arrangements without the subject's consent to capture, intercept, broadcast, and record speech made in private or confidential places, whether public or private.

Algeria sought to address the legal vacuum by strengthening its legislative system, especially since 2009, when Law No. 09-04 concerning the special rules for the prevention and combating of crimes related to information and communication technology was issued on August 5, 2009. (Law No. 09-04, 2009)

This law also contained 19 articles distributed over 6 chapters derived from international agreements international (Budapest Convention, 2001), and this law is in line with national legislation, especially those related to combating corruption, money laundering, and terrorism financing, as this law stipulates the establishment of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technology.

1-A Within the framework of Law 09-04

Digital transformation is considered one of the most important features of the current era, on one hand, and on the other hand, it makes it susceptible to risks such as hacking, exploitation,

and espionage. Therefore, it has become urgent to study the aspects of criminal protection for this data within the framework of digital transformation and the spread of artificial intelligence technologies to ensure the security and safety of this data. Additionally, determining which data should be protected under criminal law is extremely difficult because this data cannot be restricted due to the diversity and multiplicity of data types, the greatest difficulty lies in determining what can be published and generalized, and what is the opposite, and when it becomes criminal to do so the inability to establish a clear standard for distinguishing between authorized and protected information makes the picture unclear for all citizens according to the details and texts of Law 04-09¹⁰, the first chapter included general provisions and clarified the purpose of the law is to establish specific rules to prevent and combat crimes related to information and communication technologies. This means forming the basis for the automated processing of data as stipulated in the Penal Code and any other crime that incites or facilitates its use in an information system, electronic communication system, or any other system, using the data mechanism being implemented. For a specific program, information programs are defined as any process of presenting facts, information, or concepts in a form ready for processing in an information system. The legislator also addressed the concept of electronic communications, which includes any transmission or reception of signals, writings, images, or sounds by electronic means or voices or different information by any electronic means. The legislator has limited the scope of this law in consideration of the laws that ensure the confidentiality of correspondence.

And the freedom of societies in terms of the requirements of public order and the necessities of investigations or inquiries as outlined in the provisions of the Criminal Procedure Code¹¹. The second chapter of the law addresses the subject of monitoring electronic communications and the cases in which electronic monitoring may be used to prevent acts considered terrorist, sabotage, or crimes affecting state security. In the event of information being available about a potential attack on an information system in a manner similar to that which threatens public order, national defense, or state institutions.

the national economy, within the framework of the law and with written permission from the competent judicial authority. Finally, the legislator clarified in Chapter Five the name of the authority and its competencies, as it is a national body for preventing and combating crimes related to information and communication technologies. It specifically undertakes the activation and coordination of operations to prevent and combat crimes linked to information and communication technology, and assist the judicial authorities.

Where the judicial police services are responsible for investigating crimes related to information and communication technologies¹².

¹⁰ Law No. 09-04 dated 14 Sha'ban 1430, corresponding to August 5, 2000. It includes specific rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette No. 27, dated 16/08/2009.

¹¹ Code of Criminal Procedure. Order No. 155- 66 dated 18 Safar 1386 corresponding to 2, amended and supplemented by Law No. 13-23 dated August 5, 2023. Official Gazette No. 52.

¹² According to the provisions of articles 12, 12, 15, 02, 02 of law 04-09. The previous source.

2-2 Achieving digital sovereignty

Algeria has made tremendous efforts to reach the readiness of the National Digital Transformation Strategy project, which generally aims to change the digital management style and preserve the information and data of Algerians, especially in the field of investment in the financial and banking sector to realize the infrastructure axis. This was crowned with the signing, last April, of the deal related to the establishment of the Algerian National Center for Digital Services between the High Commission for Digitalization and the "Huawei Consortium" in the capital and Blida.

The project aims to achieve digital sovereignty and work on localizing national information by relying on a national information system that includes the national interoperability platform, which will connect sectoral information systems, as well as the national database and the national interactive portal for digital services that includes 40 digital public services for the benefit of citizens and institutions.

The government is currently making steady and serious strides towards digitizing all sectors, with a focus on the financial and banking sector, in line with the commitment of President Abdelmadjid Tebboune, which states, "Achieving digital transformation to improve communication and generalize the use of information technology, especially in public facility administrations, and improving the governance of the economic sector, in line with global technological developments supported by digital transformation and artificial intelligence technology, such as the reliance on blockchain technology."¹³

Algeria is considered one of the Arab countries that work on preserving its digital sovereignty, at a time when there are individual actions and programs for each country, awaiting a unified stance in the field of communications and data security protection. This will emerge from the meeting in Saudi Arabia, where there will be a unified vision for protection and communications, and later a program to empower Gaza, Sudan, and Arab countries still in a state of war, including those that have lost their right to communications, internet, and high-speed data. At the same time, the Arab League is betting on Algeria's proposals in the field of infrastructure to achieve comprehensive and purposeful connectivity in the Arab region.

Algeria possesses several factors that make it competitive for the highest regional and international ranks. The political will from the President of the Republic, who has made the dissemination of modern communication technologies and the digitization of government services one of the key pillars of his ambitious program to revive Algeria's economy, has been a significant contributor.

"In Algeria, we find no meaning in technology if it is not available to everyone regardless of social status or geographical location. What the country has achieved in terms of connecting to the fiber optic network and in terms of generalizing access for families, individuals, and institutions to fixed or mobile internet is evidence of this direction we believe in," he stated the

¹³ Al-Fatis, Muhammad bin Saeed, National Sovereignty in the Era of Virtual Geography, research published at the following link: <http://www.google.com/amp/s/.annabaa.org/arabic/informatics>



first phase will also see the commissioning of the first national data center with all its components, including the infrastructure, interoperability platform, national public service database, interactive public service portal, and national cloud. During this period, 14 fully digital public services will be put into operation.

The second phase is expected to be enhanced by the commissioning of the second national data center with all its components and infrastructure, including the interoperability platform, the national public service database, the interactive public service portal, and the national cloud. This will occur three months after the first national data center becomes operational, launching 26 fully digital public services.

The implementation of these steps involves the creation of an infrastructure consisting of two national data centers that meet the approved standards, with the aim of hosting and centralizing national data within the national territory.

This project is the first of its kind in Algeria in terms of the set objectives, its execution, scale, and the technologies used in its components.

The goal is to improve the transfer of skills and expertise in the field of executing such high-tech projects. Especially since some stages of its implementation will enable the involvement of digitalization actors and Algerian economic partners, allowing them to benefit from expertise in this field.

Algeria has made significant strides in the digital transformation process, which is expected to eliminate bureaucracy, adopt transparency in public administration, and strengthen the foundations of electronic governance, embodying the principle of digital national sovereignty. These rapid steps are a manifestation of President Abdelmadjid Tebboune's commitment, number 25, which states "achieving a digital transformation to improve communication and generalize the use of information and communication technologies, especially in public service administrations, and improving the governance of the economic sector." In September, the President established the High Commission for Digitalization, which reflects—according to experts—the importance the President places on the process in his evaluation of a presentation on digital transformation in Algeria during a cabinet meeting last Tuesday, the President of the Republic praised the "clarity of the vision for Algeria's digital direction," reminding that "the main goal of this massive project is to eliminate the bureaucracy that hinders projects, adopt transparency in managing public affairs, and accurately determine the country's needs in all sectors."

The High Commission for Digitalization, a public institution of a special nature under the supervision of the Presidency of the Republic and endowed with legal personality and financial independence, is responsible for ensuring the monitoring and implementation of the national digitalization strategy.

It is also responsible for ensuring the alignment of the digitization plans of the relevant sectors with the national digitization strategy, evaluating the achievements of each sector, and proposing necessary corrections. Additionally, it undertakes the identification of priority projects and strategic investments, the mobilization of human resources, and the financial tools specific to them. It also proposes regulatory and legal tools and/or any technical solution to

ensure the effectiveness and continuous improvement of the digital transformation axes, and suggests any measures that would enhance digital sovereignty and develop the national product in this context, the High Commission for Digitalization launched national workshops on preparing the national digital transformation strategy, where participants confirmed that the efforts of public authorities to establish a national strategy in this field would achieve digital sovereignty, which is an urgent need in today's world. In the same context, the Council of Ministers, which met the day before yesterday, approved the project to create a "base for storing and protecting electronic data by the Chinese company Huawei."

The strategy is also expected to be reinforced by a specific law on digitalization, which the High Commissioner for Digitalization, Mariem Ben Mouloud, confirmed her body is currently preparing the draft of this text, highlighting that it will be ready during the first quarter of the next year as the regulatory framework for the field of digitalization.

These rapid steps are a manifestation of President Abdelmadjid Tebboune's commitment, number 25, which states "achieving a digital transformation to improve communication and generalize the use of information and communication technologies, especially in public service administrations, and improving the governance of the economic sector." In September, the President established the High Commission for Digitalization, which reflects—according to experts—the importance the President places on the process.

In his evaluation of a presentation on digital transformation in Algeria during a cabinet meeting, the President of the Republic praised the "clarity of the vision for Algeria's digital direction," reminding that "the main goal of this massive project is to eliminate the bureaucracy that hinders projects, adopt transparency in managing public affairs, and accurately identify the country's needs in all sectors."

The High Commission for Digitalization, a public institution of a special nature under the supervision of the Presidency of the Republic and endowed with legal personality and financial independence, is responsible for ensuring the follow-up and implementation of the national digitalization strategy it is also responsible for ensuring the alignment of the digitization plans of the relevant sectors with the national digitization strategy, evaluating the achievements of each sector, and proposing the necessary corrections. Additionally, it undertakes the identification of priority projects and strategic investments, the mobilization of human resources, and the financial tools specific to them. It also proposes regulatory and legal tools and/or any technical solution to ensure the effectiveness and continuous improvement of the digital transformation axes, and suggests any measures that would enhance digital sovereignty and develop the national product in this context, the High Commission for Digitalization launched national workshops on preparing the national digital transformation strategy, where participants confirmed that the efforts of public authorities to establish a national strategy in this field would achieve digital sovereignty, which is an urgent need in today's world. In the same context, the project to create a "base for storing and protecting electronic data by the Chinese company Huawei" was approved.

The strategy is also expected to be reinforced by a specific law on digitization, which the Minister of the High Commission for Digitization, Mariam Ben Mouloud, confirmed her

agency is currently preparing the draft of this text, highlighting that it will be ready during the first quarter of the next year as the regulatory framework for the field of digitization.

Ben Mouloud explained that "the ultimate goal of digitization lies in establishing a new model for managing administrations, bodies, and public and economic institutions by transitioning from traditional paper-based management to digital governance, which primarily relies on the extensive use of modern digital technologies to enhance transparency principles, strengthen the relationship between the administration and the citizen, and facilitate transactions and administrative procedures by ensuring the provision of high-quality, secure, and fast public services at the lowest cost." establishing this would achieve a synergy in human and material resources, rationalize state expenditures, reinforce the foundations of electronic governance, and embody the principle of digital national sovereignty.

Conclusion:

This study has highlighted the growing importance of digital sovereignty in an increasingly interconnected digital environment. It has shown that digital sovereignty is not limited to technological independence, but encompasses political, economic, legal, and technological dimensions. The expansion of the Internet, digital platforms, data flows, and artificial intelligence has challenged traditional forms of state control, making the protection of critical data, infrastructures, and technologies an essential strategic concern.

Accordingly, strengthening digital sovereignty requires coherent national strategies that combine technological capacity, cybersecurity, appropriate regulation, human capital, and international cooperation. Digital sovereignty should therefore be understood not as isolation from the global digital system, but as the capacity of states to protect their strategic interests, make informed technological choices, and participate effectively in the digital economy.

Findings:

1. The study finds that digital sovereignty encompasses interconnected political, economic, technological, legal, and institutional dimensions. Its effectiveness therefore depends on the coherence between technological capabilities, regulatory capacity, economic resources, and institutional preparedness.
2. The growing cross-border circulation of data, the global operation of digital platforms, dependence on foreign technologies and infrastructures, and the expansion of artificial intelligence and cloud computing have reduced the ability of states to exercise control over digital activities solely through traditional territorial mechanisms.
3. The ability to develop, maintain, and secure critical digital infrastructures, strengthen national expertise, and build capacities in strategic fields such as cybersecurity, big data, and artificial intelligence is essential for reducing vulnerabilities and preserving national control over critical digital assets.
4. The study concludes that strengthening sovereignty in the digital domain does not imply withdrawal from the international digital system. On the contrary, states need effective regulatory frameworks, regional coordination, international cooperation, and common standards to address transnational cyber risks, protect rights, and support sustainable digital development.



Recommendations:

1. States should adopt integrated strategies that identify critical digital assets, assess technological dependencies, establish strategic priorities, and coordinate legal, economic, technological, and institutional measures within a unified national framework.
2. Greater investment should be directed toward resilient digital infrastructures, cybersecurity capabilities, research and development, artificial intelligence, data technologies, and the training of specialized human resources in strategically important digital fields.
3. National legislation should continuously evolve to address data protection, cybersecurity, digital infrastructure, artificial intelligence, digital platforms, and cross-border data flows, while maintaining an appropriate balance between security, innovation, economic development, and fundamental rights.
4. Given the transnational nature of the digital environment, states should strengthen cooperation in cybersecurity, information sharing, technical standards, digital regulation, and capacity building while preserving their ability to make strategic decisions concerning critical digital assets and technologies.

Future Research Perspectives:

Future studies could focus on developing practical indicators for measuring digital sovereignty and comparing national experiences across different regions. Further research could also examine the impact of artificial intelligence, cloud computing, digital platforms, and cross-border data flows on national digital autonomy, as well as the relationship between digital sovereignty, innovation, economic development, and international digital cooperation.

Bibliography

1. Al-Fatis, Muhammad bin Saeed. "National Sovereignty in the Era of Virtual Geography." Research published at: <http://www.google.com/amp/s/.annabaa.org/arabic/informatics>
2. Assemblée nationale, France. *Souveraineté numérique*. France, 2009.
3. Code of Criminal Procedure. Order No. 66-155 dated 18 Safar 1386, corresponding to June 8, 1966, as amended and supplemented, including by Law No. 23-13 dated August 5, 2023. *Official Gazette*, No. 52.
4. Favoreu, Louis. "Constitutional Law: Law of the Constitution and Constitution of the Law." *French Review of Constitutional Law*, no. 1 (1990): 79.
5. Ghernaouti, Solange. "Comment lutter contre la cybercriminalité." *Pour la Science*, no. 391 (May 2010): 24–27.
6. Guichet, Yves. *Constitutional Law*. Paris: Ellipses, 1996.
7. Kempf, Olivier. *Introduction à la cyberstratégie*. 2nd ed. Paris: Economica, 2015.
8. Law No. 09-04 of 14 Sha'ban 1430, corresponding to August 5, 2009, containing specific provisions relating to the prevention and combating of offences connected with information and communication technologies. *Official Gazette*, No. 47, August 16, 2009.
9. Rousseau, Dominique. "The Constitution or Politics Differently." *Débat*, no. 64 (March 1991): 183.



10. Türk, Pauline. “Définition et enjeux de la souveraineté numérique.” *Les Cahiers français*, no. 415 (May–June 2020): 18.
11. Türk, Pauline. “L’autodétermination informationnelle : un droit fondamental émergent ?” *Dalloz IP/IT*, no. 11 (November 2020): 616–620.