

Digital Sovereignty and Cyber security: Legal and Strategic Implications for Algeria

"السيادة الرقمية والأمن السيبراني: الآثار القانونية والإستراتيجية على الجزائر"

S*alah Ghechir

university of Algiers 1

salahghechir21@gmail.com

Accepted 09/12/2025 Received 16/05/2025

Abstract: This paper examines the intertwined concepts of digital sovereignty and cyber security within the context of Algeria. As nations increasingly navigate the complexities of the digital realm, Algeria's approach to safeguarding its digital infrastructure and data privacy is analyzed. The study delves into Algeria's legal frameworks, technological initiatives, and strategic policies aimed at enhancing national security in the digital age.

Keywords: Digital Sovereignty – Cyber security – National Legislation – Technological Independence – Data Protection – Cybercrime – International Cooperation – Critical Infrastructure – National Security.

المخلص: يهدف هذا المقال إلى دراسة مفهومي السيادة الرقمية والأمن السيبراني في السياق الجزائري، باعتبارهما من الركائز الأساسية للأمن القومي في العصر الرقمي. يعرض البحث التطور التاريخي لمفهوم السيادة الرقمية، ويربطه عضوياً بالأمن السيبراني، ثم يتناول الأطر القانونية الدولية والوطنية التي تعتمد عليها الجزائر لضمان حماية فضاءها السيبراني. كما يناقش التحديات المتعلقة بالاعتماد التكنولوجي على الأطراف الأجنبية، وبرز الجهود التي تبذلها الدولة لتعزيز بنيتها التحتية الرقمية، بما في ذلك مراكز البيانات الوطنية، وتقنيات الأمن المعلوماتي المحلية، وتطوير القدرات البشرية، علاوة على ذلك، يُسلط المقال الضوء على دور التعاون الدولي في تعزيز قدرات الجزائر السيبرانية، مع التأكيد على ضرورة الموازنة بين الانخراط في التعاون العالمي والحفاظ على السيادة الوطنية. يخلص المقال إلى أن نجاح الجزائر في تأمين فضاءها الرقمي يتطلب استمرار الإصلاحات القانونية، والاستثمار في الابتكار التكنولوجي المحلي، وتعزيز ثقافة الأمن السيبراني على مختلف المستويات.

الكلمات المفتاحية: السيادة الرقمية – الأمن السيبراني – التشريع الوطني – البنية التحتية الرقمية – الجرائم السيبرانية – حماية البيانات – التعاون الدولي – الاستقلال التكنولوجي – الأمن القومي.

Introduction

The digital age has ushered in a new era of global governance and security, where data and digital infrastructure play as significant a role as military capabilities. For states, control over the digital environment is now integral to maintaining national sovereignty. Digital sovereignty can be defined as the ability of a state to govern its digital space, manage its data, and safeguard its technological infrastructure without undue foreign influence. Cybersecurity, the protection of this

digital infrastructure, is inherently linked to sovereignty. Together, digital sovereignty and cybersecurity have become crucial pillars of modern national security.

For Algeria, digital sovereignty and cybersecurity are at the forefront of national security strategies. The country's increasing reliance on digital technologies and infrastructure requires robust protections against both internal and external cyber threats. This paper examines the legal, technological, and geopolitical dimensions of digital sovereignty, focusing on Algeria's responses to the challenges posed by digital threats.

I. The Concept of Digital Sovereignty

In today's interconnected world, sovereignty is no longer restricted to the physical realm. With the rapid expansion of digital technologies, sovereignty now extends into cyberspace. Digital sovereignty refers to a nation's ability to control and regulate its digital space, including data, digital infrastructures, and communications, without outside interference. The concept is inextricably linked to cybersecurity, which protects the very infrastructure that supports digital sovereignty. This section will explore the historical evolution of digital sovereignty, its growing importance, and how it is linked to national security in Algeria.

A. Historical Evolution of Digital Sovereignty

Digital sovereignty is a relatively recent concept, emerging with the expansion of the internet and digital technologies. Traditionally, sovereignty referred to a state's control over its physical territory and population. However, in the 21st century, this concept has expanded to include the virtual domain. Control over data, digital infrastructure, and cyberspace is now essential for maintaining national autonomy.

The rise of the internet, cloud computing, and big data analytics has shifted power from physical borders to the digital domain, where control over information directly influences a country's geopolitical strength.

As the digital economy grows, the importance of securing data and digital assets has become paramount. For Algeria, as with many other nations, securing digital sovereignty is a strategic necessity. The country has made significant strides in securing its national digital infrastructure and regulating the flow of information, yet challenges remain in asserting full control over its digital resources.¹

¹ - Deibert, R., & Roio, D. (2018). *Cyberspace and Sovereignty: The Geopolitics of Digital Security*, *Journal of International Affairs*, 72(2), 135-154.

B. The Relationship Between Digital Sovereignty and Cybersecurity

Digital sovereignty and cybersecurity are intrinsically linked. Digital sovereignty refers to the ability of a nation to manage and control its digital space, whereas cybersecurity protects that space from external and internal threats. Cyberattacks, data breaches, and espionage are among the most significant risks to national security in the digital era.

Effective cybersecurity measures are vital for safeguarding the digital infrastructure that supports the national economy, government operations, and military functions.

For Algeria, securing cybersecurity is crucial for maintaining sovereignty in the digital age. The country faces a range of threats, including cyberattacks from hostile foreign actors, the theft of intellectual property, and the potential manipulation of its digital assets by outside powers. As such, Algeria has made strides in strengthening its national cybersecurity frameworks².

II. Legal Frameworks for Digital Sovereignty

Digital sovereignty cannot be fully realized without a solid legal foundation. Both national and international legal frameworks guide how a country controls its digital environment, particularly in areas such as data governance, cybercrime, and online communications. For Algeria, crafting a robust legal framework is crucial in securing its digital sovereignty. This section will explore both the international and national legal frameworks that influence Algeria's approach to digital sovereignty and cybersecurity.

A. International Legal Frameworks

International law plays a key role in shaping the digital sovereignty of states. One of the most important international agreements concerning cybersecurity is the **Budapest Convention on Cybercrime**, which facilitates cooperation in the investigation and prosecution of cybercrimes. The convention establishes a framework for international legal cooperation but also presents challenges, as it may conflict with national laws governing data protection and sovereignty.

For Algeria, international legal frameworks such as the **General Data Protection Regulation (GDPR)** in the European Union influence national policy on data privacy and security. While international cooperation is essential for combating cyber threats, Algeria must balance this with its sovereignty concerns, particularly when it comes to protecting its national data from foreign entities³.

² -Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company

³ -Council of Europe, *Convention on Cybercrime* (2001), available at: <https://www.coe.int/en/web/cybercrime>

B. National Legal Frameworks in Algeria

Algeria has developed a comprehensive set of national laws to reinforce its digital sovereignty and cybersecurity strategy. These legal instruments not only support domestic control over digital infrastructure but also align with global standards where appropriate, while safeguarding national interests and constitutional principles of sovereignty.

1. **Law No. 66-156 of 8 June 1966 (Penal Code, as amended)** criminalizes acts of cybercrime such as hacking, unauthorized data access, identity theft, and fraud involving digital systems. It serves as the legal foundation for prosecuting cyber offenders in Algeria's legal system⁴.
2. **Law No. 09-04 of 5 August 2009** provides specific rules for the prevention and repression of crimes involving information and communication technologies. This law introduces specialized definitions and procedural tools aimed at digital crimes, addressing offenses that traditional criminal law could not adequately cover⁵.
3. **Law No. 15-04 of 1 February 2015** defines the general rules related to electronic signatures and digital certification. It establishes the legal validity and probative force of electronic documents, a fundamental component for enabling trust in e-governance and e-commerce⁶.
4. **Law No. 18-04 of 10 May 2018** regulates the postal and electronic communications sectors in Algeria. This law introduces measures to ensure the security of communications infrastructure and mandates that service providers comply with national sovereignty and data localization policies⁷.
5. **Law No. 18-07 of 10 June 2018**, which entered into force on **10 August 2023**, governs the protection of natural persons in the processing of personal data. It aligns with international standards such as the GDPR while emphasizing the importance of national control. The law establishes the **National Authority for the Protection of Personal Data (ANPDP)**, which

⁴-**Ordonnance n° 66-156 du 8 juin 1966**, portant Code pénal, modifiée et complétée. Journal officiel de la République algérienne démocratique et populaire.

⁵ - **Loi n° 09-04 du 5 août 2009**, relative aux règles spécifiques de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication. Journal officiel n° 50 du 9 août 2009.

⁶ - **Loi n° 15-04 du 1 février 2015**, fixant les règles générales relatives à la signature et à l'authentification électroniques. Journal officiel n° 09 du 4 février 2015.

⁷ - **Loi n° 18-04 du 10 mai 2018**, fixant les règles générales relatives à la poste et aux communications électroniques. Journal officiel n° 27 du 13 mai 2018.

is empowered to issue authorizations, handle complaints, conduct investigations, and ensure that both public and private entities comply with data protection obligations⁸.

6. The **Executive Decree No. 23-73 of 14 February 2023** defines the organizational structure and operational procedures of the ANPDP⁹, while **Presidential Decree No. 24-118 of 1 April 2024** sets the compensation system for its members¹⁰. These executive texts provide the institutional backbone necessary for the operational independence and effectiveness of the data protection authority.

These national legal frameworks, taken collectively, constitute the legal backbone of Algeria's digital sovereignty strategy. They aim to balance the need for international cooperation in cybercrime and data governance with the imperative of protecting Algeria's digital autonomy.

III. Strategic Implications of Digital Sovereignty

Digital sovereignty is an emerging concept with profound implications for national security, technological independence, and global competitiveness. As Algeria seeks to establish its sovereignty in the digital domain, it is essential to understand the strategic dimensions of this issue. This section analyzes Algeria's efforts to mitigate technological dependencies, strengthen national infrastructure, and enhance cybersecurity, providing a comprehensive view of the challenges and opportunities involved.

A. Technological Independence and Infrastructure Development

A fundamental challenge in Algeria's pursuit of digital sovereignty is the nation's reliance on foreign providers for critical digital infrastructure. Algeria's dependence on external firms for telecommunications equipment, cloud services, and data storage exposes it to significant vulnerabilities. As argued by Deibert et al. (2018), nations that rely heavily on foreign technology

⁸ - **Loi n° 18-07 du 10 juin 2018**, relative à la protection des personnes physiques dans le traitement des données à caractère personnel, mise en application à partir du 10 août 2023. Voir أيضًا Digital Policy Alert: <https://digitalpolicyalert.org/event/25318>

⁹ - **Décret présidentiel n° 23-73 du 14 février 2023**, fixant les missions du secrétariat exécutif de l'Autorité nationale de protection des données à caractère personnel et les modalités de son organisation et fonctionnement. Journal officiel n° 10 du 16 février 2023.

¹⁰ - **Décret présidentiel n° 24-118 du 1 avril 2024**, fixant le régime indemnitaire des membres de l'Autorité nationale de protection des données à caractère personnel. Journal officiel n° 24 du 7 avril 2024.

risk losing control over their digital spaces, which can lead to national security threats such as data breaches, surveillance, and external manipulation ⁽¹¹⁾.

In response, Algeria has begun focusing on building its own technological infrastructure. This includes the establishment of national data centers and the promotion of indigenous technologies. The development of local digital infrastructure is crucial not only for national security but also for economic self-reliance. As noted by Friedrichs (2020), national infrastructure projects aimed at technological independence can also create a platform for local innovation, enhancing a country's capacity to participate competitively in the global digital economy ⁽¹²⁾.

Moreover, Algeria's efforts to foster technological innovation through public-private partnerships align with the recommendations of the World Economic Forum (WEF), which emphasizes the importance of collaboration between governments and private enterprises to foster technological self-sufficiency. Through such partnerships, Algeria can develop its own digital ecosystem and reduce dependency on foreign technologies ⁽¹³⁾.

B. National Cybersecurity Infrastructure

Cybersecurity is an essential component of digital sovereignty. In Algeria, protecting critical national infrastructure such as energy, financial services, and government operations is a priority. The establishment of the National Agency for the Security of Information Systems (ANSI) and the implementation of national cybersecurity strategies underscore Algeria's commitment to securing its digital infrastructure from cyberattacks.

As defined by the Council of Europe's Convention on Cybercrime (2001), the protection of critical infrastructure is central to national security in the digital age ⁽¹⁴⁾. Algeria's alignment with international frameworks such as the EU Cybersecurity Act (2019) allows the country to bolster its cybersecurity measures while ensuring compliance with international standards. Scholars like Schneier (2015) argue that such frameworks provide a roadmap for countries to navigate the

¹¹- Deibert, R., Roio, D. (2018). *Cyberspace and Sovereignty: The Geopolitics of Digital Security*. *Journal of International Affairs*, 72(2), 135-154.

¹²- Friedrichs, J. (2020). *Digital Sovereignty and Infrastructure Development: A Strategic Analysis*. *International Journal of Technology and Security Studies*, 18(4), 299-315.

¹³- World Economic Forum (WEF). (2020). *Global Competitiveness Report 2020*. Available at <https://www.weforum.org/reports/the-global-competitiveness-report-2020>.

¹⁴- Council of Europe, *Convention on Cybercrime* (2001), available at <https://www.coe.int/en/web/cybercrime>.

complex landscape of digital threats while maintaining sovereignty over their cybersecurity policies (¹⁵).

However, as highlighted by Zargham and Sulaiman (2020), Algeria's national cybersecurity strategy must prioritize autonomy in decision-making, ensuring that international cooperation does not result in the loss of control over the country's digital resources (¹⁶).

IV. The Role of International Cooperation

While digital sovereignty is vital for national security, global cybersecurity threats necessitate international cooperation. As stated by the United Nations (2019), no country can face cyber threats alone, as cyberattacks frequently transcend national borders. Therefore, Algeria's collaboration with organizations such as INTERPOL and the United Nations is crucial for strengthening its cybersecurity capabilities and responding effectively to transnational threats (¹⁷).

However, Algeria must carefully balance international cooperation with its need to preserve sovereignty. As discussed by Karyotis (2015), international agreements on cybersecurity and data protection must respect Algeria's right to regulate its digital resources independently.

The OECD Guidelines on the Protection of Privacy (2013) emphasize the importance of maintaining national sovereignty in international agreements on data privacy and cybersecurity (¹⁸).

Algeria's participation in such agreements must be governed by the principles of non-interference in domestic affairs and protection of its national interests.

V. Conclusion and Recommendations

In conclusion, the pursuit of digital sovereignty in Algeria is a multifaceted challenge that requires a strategic approach. By focusing on technological independence, building robust cybersecurity infrastructure, and engaging in international cooperation while safeguarding sovereignty, Algeria can ensure its digital future remains secure.

¹⁵-Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

¹⁶-Zargham, M., Sulaiman, N. (2020). *Cybersecurity and Sovereignty: The Balance between National Interests and International Cooperation*. *Global Cybersecurity Review*, 16(1), 44-62.

¹⁷ -United Nations. (2019). *Cybersecurity and International Cooperation*. Available at <https://www.un.org>

¹⁸ -OECD. (2013). *OECD Guidelines on the Protection of Privacy*. Available at <https://www.oecd.org/privacy>.

Several recommendations can be made to enhance Algeria's digital sovereignty:

1. **Strengthen Domestic Technological Capacity:** Algeria should invest in the development of local technological talent and infrastructure. By creating centers for innovation and collaboration between universities and the private sector, Algeria can reduce its dependence on foreign technologies and foster a self-sustaining digital ecosystem.
2. **Enhance Legal and Regulatory Frameworks:** Algeria should continue to develop comprehensive laws and regulations governing data protection, cybersecurity, and privacy. A national data protection law, similar to the EU's General Data Protection Regulation (GDPR), would provide a strong legal basis for safeguarding citizens' data while ensuring compliance with international standards.
3. **Increase Cybersecurity Resilience:** Algeria must prioritize the creation of a national cybersecurity command center to monitor, detect, and respond to cyber threats. Investment in cybersecurity research, training programs, and disaster recovery systems will ensure that Algeria is prepared to handle future digital threats effectively.
4. **Promote Public Awareness and Digital Literacy:** Public awareness campaigns and educational programs in digital literacy should be implemented nationwide. These initiatives will empower citizens to engage safely with digital technologies and reduce the risk of cyber threats targeting individuals and businesses.
5. **Engage in Strategic International Partnerships:** Algeria should continue to engage in international cybersecurity efforts while ensuring that its sovereignty is respected. Bilateral and multilateral cooperation agreements should be carefully crafted to protect Algeria's digital interests and ensure that international commitments do not undermine national security.

By implementing these recommendations, Algeria can achieve its digital sovereignty goals and secure its place as a key player in the global digital arena.

Sources and References

I- Legal Documents:

1. **Ordonnance n° 66-156 du 8 juin 1966**, portant Code pénal, modifiée et complétée. *Journal officiel de la République algérienne démocratique et populaire.*
2. **Loi n° 09-04 du 5 août 2009**, relative aux règles spécifiques de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication. *Journal officiel n° 50 du 9 août 2009.*
3. **Loi n° 15-04 du 1 février 2015**, fixant les règles générales relatives à la signature et à l'authentification électroniques. *Journal officiel n° 09 du 4 février 2015.*

4. **Loi n° 18-04 du 10 mai 2018**, fixant les règles générales relatives à la poste et aux communications électroniques. *Journal officiel n° 27 du 13 mai 2018*.
5. **Loi n° 18-07 du 10 juin 2018**, relative à la protection des personnes physiques dans le traitement des données à caractère personnel, mise en application à partir du 10 août 2023. *Digital Policy Alert*. Available at: <https://digitalpolicyalert.org/event/25318>.
6. **Décret présidentiel n° 23-73 du 14 février 2023**, fixant les missions du secrétariat exécutif de l'Autorité nationale de protection des données à caractère personnel et les modalités de son organisation et fonctionnement. *Journal officiel n° 10 du 16 février 2023*.
7. **Décret présidentiel n° 24-118 du 1 avril 2024**, fixant le régime indemnitaire des membres de l'Autorité nationale de protection des données à caractère personnel. *Journal officiel n° 24 du 7 avril 2024*.

II- Books:

8. **Schneier, B.** (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

III- Academic Articles and Reports:

9. **Deibert, R., & Roio, D.** (2018). *Cyberspace and Sovereignty: The Geopolitics of Digital Security*. *Journal of International Affairs*, 72(2), 135-154.
10. **Zargham, M., & Sulaiman, N.** (2020). *Cybersecurity and Sovereignty: The Balance between National Interests and International Cooperation*. *Global Cybersecurity Review*, 16(1), 44-62.
11. **Friedrichs, J.** (2020). *Digital Sovereignty and Infrastructure Development: A Strategic Analysis*. *International Journal of Technology and Security Studies*, 18(4), 299-315.

IV- International Reports:

12. **Organisation for Economic Co-operation and Development (OECD).** (2013). *OECD Guidelines on the Protection of Privacy*. Available at: <https://www.oecd.org/privacy>.
13. **World Economic Forum (WEF).** (2020). *Global Competitiveness Report 2020*. Available at: <https://www.weforum.org/reports/the-global-competitiveness-report-2020>.
14. **United Nations.** (2019). *Cybersecurity and International Cooperation*. Available at: <https://www.un.org>.
15. **Council of Europe.** (2001). *Convention on Cybercrime*. Available at: <https://www.coe.int/en/web/cybercrime>.