DOI: https://doi.org/10.36719/2706-6185/56/68-74

Ezzine Abdelhak
University of Kasdi Merbah Ouargla, Algeria
https://orcid.org/0000-0002-6529-9344
ezzine.abdelhak@univ-ouargla.dz
Toumi Fadilha
University of Kasdi Merbah Ouargla, Algeria
https://orcid.org/0000-0003-1078-2512
toumi.fadila@univ-ouargla.dz

Enhancing Digital Immunity in Algeria: An Integrated Analysis of Legislative, Technical, and Institutional Safeguards Against Cyber Threats

Abstract

Algerian society has witnessed a significant increase in the use of information and communication technologies, accompanied by the widespread adoption of various digital applications. This growing digital engagement has highlighted the urgent need to strengthen digital protection systems, particularly regarding personal data, given its high sensitivity in the face of rising cyberattacks and security breaches and their multifaceted negative consequences. Based on these considerations, this article aims to shed light on Algeria's efforts to enhance digital immunity by examining the initiatives and measures undertaken at the legislative, technical, and institutional levels.

Keywords: *digital immunity, cyber threats, legislative technical safeguards, institutional capacity, Algeria*

Ezzine Abdelhak
Kasdi Merbah Ouargla Universiteti, Əlcəzair
https://orcid.org/0000-0002-6529-9344
ezzine.abdelhak@univ-ouargla.dz
Toumi Fadilha
Kasdi Merbah Ouargla Universiteti, Əlcəzair
https://orcid.org/0000-0003-1078-2512
toumi.fadila@univ-ouargla.dz

Əlcəzairdə rəqəmsal immunitetin gücləndirilməsi: Kiber təhdidlərə qarşı qanunvericilik, texniki və institusional təhlükəsizlik tədbirlərinin inteqrasiya edilmiş təhlili

Xülasə

Əlcəzair cəmiyyəti informasiya və kommunikasiya texnologiyalarının istifadəsində əhəmiyyətli dərəcədə artımın şahidi olub və müxtəlif rəqəmsal tətbiqlərin geniş yayılmasına səbəb olub. Bu artan rəqəmsal iştirak, artan kiberhücumlar və təhlükəsizlik pozuntuları və onların çoxşaxəli mənfi nəticələri qarşısında yüksək həssaslığı nəzərə alınmaqla, xüsusilə şəxsi məlumatlarla bağlı rəqəmsal mühafizə sistemlərinin gücləndirilməsinin təcili ehtiyacını vurğulayıb. Bu mülahizələrə əsaslanaraq, bu məqalə, qanunvericilik, texniki və institusional səviyyələrdə həyata keçirilən təşəbbüsləri və tədbirləri araşdıraraq Əlcəzairin rəqəmsal immuniteti gücləndirmək səylərinə işıq salmağı hədəfləyir.

Açar sözlər: *rəqəmsal toxunulmazlıq, kibertəhdidlər, qanunvericilik texniki təhlükəsizlikləri, institusional potensial, Əlcəzair*

Introduction

Like other countries, Algeria is striving to enhance its information security in an era marked by rapid digitalization and technological advancement. Cybersecurity and digital immunity have become fundamental pillars of national security and sovereignty. Algeria is among the countries facing multiple challenges in the digital security domain, which has prompted it to undertake significant efforts to strengthen its digital immunity.

Research

This paper aims to highlight these efforts by focusing on the following objectives:

* Presenting the legal and institutional framework of cybersecurity in Algeria;
* Examining the technical infrastructure underpinning digital immunity;
* Analyzing the status of human resources trained in cybersecurity;
* Identifying the main challenges and obstacles facing Algeria in this field;
* Providing recommendations for the development of digital immunity.

The study adopts a descriptive-analytical methodology, analyzing data and information drawn from official sources and previous research. The central research question revolves around the mechanisms adopted by Algeria to strengthen its digital immunity.

1- The Concept of Digital Immunity

Digital immunity refers to an integrated set of policies and technologies that enable dynamic adaptation to evolving threats. Analogous to the biological immune system, digital immunity differs from cybersecurity in its focus and operational mechanisms:

* Cybersecurity focuses on protection from external attacks.
* Digital immunity focuses on building intrinsic resilience and self-recovery capabilities.

The mechanisms of digital immunity consist of:

* Secure-by-design infrastructures, ensuring security is embedded from the outset;
* Smart detection and response systems, often referred to as self-healing technologies;

Secure interoperability between systems to ensure coordinated and robust protection. (Lori)

2- The Various Dimensions of Digital Security

2.1- Technical and Physical Dimension

This dimension encompasses secure digital infrastructure, including robust communication networks resistant to penetration and fortified data centers that protect storage environments and operating systems. It involves the development of vulnerability-resistant systems and the deployment of advanced protection technologies such as encryption, data protection during transmission and storage, firewalls, traffic filtering, intrusion detection systems, network monitoring for attack detection, multi-factor authentication, and strengthened verification processes (Daniel & others, 2021).

2.2- Legal and Regulatory Dimension

This refers to national legislation that criminalizes unlawful cyber activities, data protection laws that regulate data collection and processing, and privacy regulations safeguarding personal information. It also includes regulatory frameworks involving technical standards, licensing and certification requirements for service providers, oversight mechanisms, and compliance monitoring (Daniel & others, 2021).

2.3- Human Dimension

The human dimension aims to build digital awareness through education and training programs, skill development initiatives, and awareness campaigns that promote a culture of security and safe digital practices. It includes:

*Cybersecurity experts: Developing specialized competencies;
* Security researchers: Identifying vulnerabilities and threats;
* Risk managers: Overseeing and managing digital risks (Daniel & others, 2021).

2.4- Organizational and Administrative Dimension

This dimension involves digital governance through policies and procedures that establish regulatory frameworks, risk management strategies (identification, assessment, and mitigation), and adherence to security standards. It includes institutional structures such as:

* Emergency response teams, to manage incidents;

*Security operations centers, for continuous monitoring;

*Security committees, for coordination and decision-making (EZZINE, Digital prevention mechanisme in emergency communiction, 2025)

2.5- Economic and Financial Dimension

Investment in security has significant implications for the national economy. This dimension involves allocating financial resources, government funding, supporting national initiatives, and encouraging private investment through cost–benefit analysis, cyber insurance to transfer financial risks, and economic incentives to encourage compliance and security innovation (Bara, 2017, p. 261).

2.6 - Social Dimension

The social dimension constitutes a cornerstone in the interaction between individuals, technology, and society. Digital trust is a defining feature, encompassing service reliability, transparency in data processing, accountability for damages, and community participation through initiatives such as:

* Community initiatives: Engaging society in protection;

* Digital volunteering: Individual contributions to security;

* Community partnerships: Collaborative efforts among stakeholders (EZZINE, Algerian effoerts in digital ummunity, 2025).

2.7 -International and Regional Cooperation Dimension

International cooperation is indispensable in combating cybercrime and protecting data security. It involves active participation in bilateral agreements, multilateral treaties, and information-sharing frameworks, including:

* Bilateral partnerships between states;

* International treaties as multilateral frameworks;

* Information-sharing initiatives on threats.

It also entails alignment with global standards through the adoption of international norms, compliance with treaties, and mutual recognition of certifications and standards (Daniel & others, 2021).

2.8- Dynamic Dimension

Information and communication technologies are evolving continuously, giving rise to new forms of applications, the latest of which involve artificial intelligence. These rapid developments bring both positive and negative consequences, which make **continuity, development, and regular updates** essential. This dimension focuses on keeping pace with technological progress and adapting to emerging threats through:

* Responding to new risks;

* Learning from past incidents to improve systems based on experience;

* Future planning by anticipating and forecasting upcoming challenges;

* Preparing for expected risks and ensuring flexibility and adaptability to change (Daniel & others, 2021).

2.9 - Ethical and Value-Based Dimension

Ethical principles form the normative foundation of digital security. They include **privacy**, by respecting individuals' personal data; **integrity**, by ensuring the accuracy and reliability of information; and **ethical responsibility**, through accountability, transparency, and clarity in procedures. This dimension also emphasizes **social responsibility**, considering the broader societal impacts of digital systems (Daniel & others, 2021).

2.10- Environmental and Sustainable Development Dimension

Digital sustainability involves optimizing energy consumption, ensuring the safe disposal of electronic waste, and monitoring the life cycles of technologies. It also includes the **design of long-term, environmentally secure systems** to protect infrastructure, secure environmental systems, and

implement long-term security technologies that ensure the continuity and resilience of digital ecosystems (EZZINE, communication of social responsablity in Algerian public institustions , 2025).

3- Algeria's Efforts to Strengthen its Digital Immunity

3.1- National Legal and Regulatory Framework

The Algerian legislator has given particular attention to the security of information systems due to the legal and security challenges brought about by technological transformations. Within this context, **Law No. 04-15 of 10 November 2004**, amending and supplementing Ordinance No. 66-156 containing the Penal Code, (Law , 2004) introduced a new section titled *"Offences Against Automated Data Processing Systems."*

This amendment was a legislative response to the rapid digital transformations and the emergence of new forms of cybercrime targeting electronic systems and digital data. In its explanatory memorandum, the legislator stressed that the spread of communication technologies led to new criminal behaviors, requiring legal intervention to protect data and information from unlawful access.

The legislator recognized that the core of any information system lies in the data processed automatically within computers, which becomes information after processing and storage. Hence, comprehensive legal protection was provided for this data—both in terms of its nature and the systems that store and process it, including information networks.

The term "offences against automated data processing systems" was deliberately chosen to limit criminalization to acts that directly target the information system itself, excluding cases where the system is merely used as a tool to commit other crimes.

3.1-National Information Systems Security Framework

The legal framework was further strengthened by **Presidential Decree No. 05-20**, which laid the foundations for the **National Information Systems Security Framework**. This framework serves as the state's tool for developing and coordinating the implementation of a national information security strategy.

✓ **The National Council for the Security of Information Systems**

The decree established the National Council for the Security of Information Systems as the highest authority responsible for planning and coordinating national digital security efforts.

Its main tasks include:

* Reviewing and approving elements of the national information security strategy;

* Endorsing the action plans and activity reports of the National Agency for Information Systems Security;

* Giving opinions on draft laws and regulations related to information security;

* Approving cooperation agreements with specialized foreign bodies;

* Validating the electronic certification policy approved by the competent national authority (Presidential Decree , 2020).

✓ **The National Agency for the Security of Information Systems (NASSI)**

The National Agency for the Security of Information Systems is a public administrative institution with legal personality and financial autonomy, headquartered in Algiers.

Its core functions include:

* Preparing the elements of the national information security strategy and submitting them to the National Council;

* Coordinating the implementation of the strategy approved by the Council;

* Developing national capabilities in cybersecurity and modern protection technologies;

* Protecting government websites from cyberattacks;

* Deploying advanced systems and software to prevent intrusions and malware;

* Training and qualifying highly skilled human resources to ensure the security of the state's information infrastructure. (law, 2018)

The rapid evolution of digital technologies and the emergence of sophisticated viruses and cyberattacks require the state to continuously update its security frameworkand rely on national technical expertise (Presidential Decree , 2020)

3.3-International Efforts to Protect Information Systems

Given the **transnational nature** of cybercrime, effective international cooperation is essential. Algeria's international efforts focus on two main areas:

✓ **Judicial Cooperation and Extradition of Cybercriminals**

The extradition of cybercriminals relies on international cooperation within the framework of treaties on mutual legal assistance in criminal matters. This allows for the prosecution of offenders who exploit geographical boundaries due to the digital nature of their crimes. International treaties also call for a **unified global convention** on the extradition of cybercriminals (Loukal, 2019).

✓ **Specialized International Conventions**

Many countries have signed international treaties to combat cybercrime, the most notable being the **Budapest Convention on Cybercrime** (signed on 23 November 2001), which remains the first and most comprehensive international treaty in this field.

Its objectives are to:

* Harmonize national legislation on cybercrime;

* Define procedural powers for collecting digital evidence and tracking offenders;

* Strengthen mechanisms for rapid and effective international cooperation among member states (George, 2013, p. 10).

4- Challenges and Obstacles

Despite the efforts made by the Algerian state to secure its information systems and establish a legal framework to combat cybercrime, practical realities reveal several persistent challenges that hinder the achievement of comprehensive and effective information security. These challenges can be summarized as follows:

4.1- Legislative and Legal Challenges

The legal framework governing information systems security in Algeria is relatively recent and therefore requires **constant updating and revision** to keep pace with the rapid evolution of technology and emerging forms of cybercrime.

Some legal provisions do not adequately address new types of cyber threats, particularly those linked to artificial intelligence, targeted cyberattacks against critical infrastructure and cyber-espionage.

Moreover, the judicial system faces difficulties in prosecuting cybercrimes due to their *technical complexity* and the challenges of collecting admissible digital evidence in accordance with legal standards.

4.2- Technical and Infrastructural Challenges

National technical capacities in information security remain limited compared to the scale and sophistication of cyber threats. Many institutions—especially public ones—still rely on **outdated systems and software** that lack regular updates, making them highly vulnerable to intrusion.

Insufficient investment in digital infrastructure and the scarcity of specialized technical expertise in cybersecurity constitute significant barriers to building a robust national security system (Qalaa Al-Droos, 2022, p. 257).

4.3-Shortage of Specialized Human Resources

The Algerian information sector suffers from a shortage of qualified human resources in areas such as cyberattack analysis, security auditing, and incident response.

This is primarily due to limited academic and technical training in information security, as well as the absence of specialized research centers in this critical field. As a result, Algeria relies heavily on foreign solutions and expertise, rather than developing autonomous national capabilities.

4.4-Institutional Coordination Gaps

Although official bodies such as the National Council for the Security of Information Systems and the National Agency for Information Systems Security exist, coordination between these entities and other public and private institutions remains limited.

This is evident in the absence of a unified national system for information-sharing, and the lack of a comprehensive national cyber emergency response plan** that brings together stakeholders from both the public and private sectors.

4.5- International Cooperation Challenges

Because cybercrime is inherently transnational, combating it requires broad and rapid international cooperation. However, international judicial cooperation mechanisms continue to face obstacles stemming from differences in national legal systems, diverse legal references, and difficulties in extraditing cybercriminals** in the absence of effective bilateral agreements.

Furthermore, Algeria has not yet officially joined some key international agreements, such as the Budapest Convention, which limits its ability to fully benefit from existing international cooperation mechanisms.

4.6-Societal Awareness Challenges

Low levels of cybersecurity awareness among users remain one of the most critical obstacles to information system protection.

Many individuals and organizations underestimate the importance of data protection and do not follow basic digital hygiene practices, such as using strong passwords or regularly updating systems.

This lack of security culture renders even well-protected systems vulnerable to human error or negligence when handling sensitive information.

Conclusion

In conclusion, the legal protection of information systems in Algeria rests on two complementary pillars:

First one is the national legal and institutional framework, based on legislative and regulatory instruments such as Law No. 04-15, Presidential Decree No. 05-20, and the establishment of the National Council and the National Agency for Information Systems Security.

Seconde one is the international dimension, grounded in cooperation and coordination with the global community through multilateral agreements, particularly the Budapest Convention on Cybercrime.

Together, these efforts form the foundation of a comprehensive national cybersecurity framework capable of keeping pace with technological evolution and countering growing digital threats.

However, Algeria continues to face a complex set of legislative, technical, human, organizational, and international challenges, which necessitate adopting an **integrated and holistic approach that involves:

Updating legal frameworks to address emerging threats;

Enhancing technical capacities through investment and modernization;

Developing national expertise via specialized training and research;

Strengthening international cooperation;

Promoting societal awareness of information security.

Without tackling these challenges collectively, the national cybersecurity framework will remain vulnerable, unable to fully keep pace with the accelerating dynamics of the digital threat landscape.

References

1. Bara, S. (2017). Cyber security in Algeria: Policies and institutions. *Algerian Journal of Human Security*, 261.
2. Daniel, B., et al. (2021). *The essential digital security guide for children*. Eyrolles.
3. Ezzine, A. (2025). *Algerian efforts in digital immunity*.
4. Ezzine, A. (2025). *Communication of social responsibility in Algerian public institutions*.
5. Ezzine, A. (2025). *Digital prevention mechanisms in emergency communication*.
6. George, L. (2013). International internet treaties: Facts and challenges. *National Defense Magazine*.
7. Law No. 04-15 of November 10, 2004, amending and supplementing Decree No. 66-156 containing the Penal Code. (2004). *Official Journal of the People's Democratic Republic of Algeria*.

8. Law No. 18-07 on the protection of natural persons in the processing of personal data. (2018). *Official Journal of the People's Democratic Republic of Algeria*.
9. Lori, P. (n.d.). Why is the digital immune system important? *Gartner*. https://www.gartner.com
10. Loukal, M. (2019). International and national legal protection of personal data in the digital space. *Journal of Legal and Political Sciences*.
11. Presidential Decree No. 20-05 of January 20, 2020, concerning the information security system. (2020). *Official Journal of the People's Democratic Republic of Algeria*, No. 5.
12. Qalaa Al-Droos, S. (2022). National cybersecurity: A reading of the most important security and technical strategies to confront cybercrime in Algeria. *Al-Rawak Journal of Social and Human Studies*.

Received: 14.05.2025
Accepted: 29.11.2025