



THE SOVEREIGNTY OF DIGITAL HEALTH: BETWEEN CYBERSECURITY THREATS AND LEGAL SAFEGUARDS

D^r. MANSOURI Touria*

Djilali Al-Yabis University - Sidi Bel
Abbes, Algeria

mansouritouria1@gmail.com

Member of the Public Utilities and
Development Laboratory.

P^r. ABBAR Omar

Djilali Al-Yabis University - Sidi Bel
Abbes, Algeria

abbar.omar@gmail.com

Member of the Public Utilities and
Development Laboratory.

Send Article Date: 07-07-2025

Date of acceptance of the article: 26-08-2025

Abstract:

This paper investigates digital health sovereignty in light of increasing cybersecurity threats and legal frameworks developed to combat them. The growing integration of digital technologies in healthcare has given rise to cybercrimes that jeopardize data integrity, confidentiality, and national control over health systems. These crimes present legal issues concerning jurisdiction, attribution, and standards of evidence. The study focuses on Algeria's legal response, especially Law No. 09/04 on cybercrime, examining its role in protecting digital health platforms. It evaluates the effectiveness of these measures and offers legal strategies to strengthen digital health sovereignty amid evolving cyber threats and emerging technological risks.

key words: Digital Health Sovereignty, Cybercrime, Cybersecurity Threats, Law No. 09/04, Legal Protection.

Introduction:

The dawn of the third millennium has witnessed a profound digital transformation, characterized by rapid advances in information exchange, scientific innovation, and the emergence of real-time communication networks. This digital shift has revolutionized individual and institutional interactions, replacing

* MANSOURI Touria

traditional systems with cyberspace-based operations. Among the sectors most impacted is healthcare, where digital technologies have enhanced service delivery but also introduced significant vulnerabilities.

The misuse of digital tools has led to a surge in cybercrimes targeting the sovereignty of digital health systems. These sophisticated attacks pose threats not only to data confidentiality but also to national control over electronic health infrastructures. This growing risk has attracted international and regional legal attention, especially in Algeria, where digital health data security has become a critical concern.

This study addresses the central research problem: Are the current Algerian legal frameworks, particularly Law No. 09/04 on cybercrime, adequate in addressing the unique challenges of cybercrimes affecting digital health sovereignty?

The research adopts a descriptive and analytical legal methodology, aiming to examine the preventive and remedial mechanisms established under Algerian law.

The study is structured around two main hypotheses:

1. Existing Algerian legislation partially addresses the complexities of cyber threats to digital health sovereignty.
2. Enhancing legal and technical frameworks is essential to ensure comprehensive digital health protection.

Accordingly, the paper is organized into two chapters:

- **Chapter One:** Challenges to Digital Health Sovereignty



- **Chapter Two:** Legal and Technical Mechanisms under Algerian Law to Combat Cybercrimes Affecting Digital Health

Chapter One: Challenges to Digital Health Sovereignty

Digital health sovereignty refers to the ability of states and healthcare institutions to exercise full control over their digital systems and health-related data without excessive reliance on external entities. It encompasses the protection of medical data, the security of electronic health transactions, and the independence of decision-making in digital health governance. Preserving such sovereignty is essential to ensure the confidentiality, integrity, and resilience of national healthcare infrastructures in the face of evolving cyber threats.

Section One: Obstacles to Achieving Digital Health Sovereignty

The widespread proliferation of cybercrime and emerging digital threats-fueled by the continuous expansion in the use of information and communication technologies across all sectors-has compelled many countries to prioritize information security. In this context, national efforts have increasingly focused on protecting the information systems of individuals, institutions, and governments from cyberattacks, intrusions, and unauthorized access.

These challenges are particularly acute in the healthcare sector, where the digitalization of services has rendered medical data and platforms especially vulnerable. Obstacles include limited national infrastructure, dependency on foreign technologies and cloud services, weak regulatory frameworks, and a shortage of specialized cybersecurity personnel in the health domain. Such constraints pose a direct risk to the sovereignty of health data and decision-making processes, undermining the trust and resilience of digital health systems. (Boudiaf, 2020, p. 178)

Section Two: Digital Threats and Protective Responses.

In the digital era, the growing integration of information and communication technologies into healthcare systems has introduced both unprecedented opportunities and significant vulnerabilities. While digital transformation enhances efficiency, accessibility, and the quality of healthcare services, it simultaneously exposes critical medical infrastructures to a wide range of cyber threats. These threats-ranging from unauthorized data breaches to sophisticated ransomware attacks-pose a direct challenge to national digital health sovereignty, jeopardizing patient privacy, institutional reliability, and the autonomy of public health governance. In response to these escalating risks, healthcare institutions and national authorities have sought to implement robust protection strategies aimed at safeguarding the confidentiality, integrity, and availability of health data. This section examines the evolving landscape of cyber threats targeting digital health systems and explores the legal, technological, and procedural safeguards adopted to counteract them. It also analyzes real-world case studies that reveal systemic vulnerabilities and inform best practices for strengthening digital health sovereignty in practice.

Subsection One: Cybercrimes Undermining Digital Health Sovereignty

Information security is a dynamic and rapidly evolving field that seeks to address the growing and emerging challenges in the digital information landscape. In recent years, hospitals and healthcare systems have become prime targets for cyberattacks, rendering patient data increasingly vulnerable to unauthorized access and exploitation.

Cybercrimes affecting the security of digital health sovereignty include a wide range of malicious acts such as unauthorized



access to health records, ransomware attacks on hospital databases, and the infiltration of digital medical infrastructure. These breaches not only threaten data confidentiality but may also result in severe consequences-such as the manipulation of medical records, fraudulent prescriptions, or even identity theft involving sensitive personal health information.

Such crimes strike at the very core of digital health sovereignty, as they erode institutional control over data and compromise the integrity and reliability of health systems. The increasing sophistication of these attacks highlights the urgent need for comprehensive legal and technological frameworks that can anticipate, prevent, and respond to cyber threats in the healthcare sector.(Guillame, 2013, p. 161)

- Cybercrimes are among the modern types of offenses committed using digital technologies, foremost among them the internet. These crimes target information systems through hacking operations with the aim of illegally altering or manipulating data.
- They are characterized by their invisible nature, as they often leave no tangible evidence, making their detection and forensic investigation particularly challenging. Moreover, they are transnational by nature, unrestricted by geographical or temporal boundaries, which further complicates the task of tracking down perpetrators.
- Additionally, most victims refrain from reporting such crimes-either because they fail to detect the breach in time, or out of fear of reputational damage-which contributes to the increasing spread of cybercrime.
- Competent authorities also face legal challenges in classifying and defining these offenses, given their highly technical nature, which requires specialized expertise in the field of information technology.(Khalil, 2017, p. 401)

Subsection Two: Protection Strategies and Case Studies in Digital Health Sovereignty

Among the key preventive measures adopted to protect against cybercrime are the following: (Saad Ghaleb, 2006, p. 226)

- **Creating Data Backups:** Regular duplication of important files ensures the recovery of data in the event of cyberattacks or system failures.
- **Using Anti-Virus Software:** These programs detect, block, and remove malicious software that may compromise the integrity of digital systems.
- **Firewall Software:** Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted internal networks and untrusted external sources.
- **Access Authentication Controls:** These include awareness and training programs for employees and system users on best security practices and how to identify potential threats.
- **Biometric Security Features:** These involve the use of physiological characteristics such as fingerprint recognition, iris scanning, and voice authentication to enhance system access security.
- **Data Encryption:** Encryption is a key security technique aimed at protecting the confidentiality of data, especially in electronic transactions executed remotely. In this context, the 1996 UNCITRAL Model Law on Electronic Commerce, issued by the United Nations Commission on International Trade Law (adopted on June 12, 1996, and endorsed by General Assembly Resolution No. 51/162 on December 16, 1996), addressed the use of electronic signatures and defined electronic encryption as a branch of



applied mathematics. It involves converting a readable message into an unintelligible form, and subsequently restoring it to its original state.(Kadri & Meklekal, 2022, pp. 7–8)

- The hospital may provide the attending physician with access to the administrative office or assign a medical secretary to receive and record medical reports specific to each physician.
- Alternatively, the medical team may prepare and record patient data themselves, a practice that is particularly suitable for small-sized hospitals where administrative support is limited.

Amid the rising wave of cyberattacks targeting healthcare systems, this applied study examines the state of digital health sovereignty through a comparative analysis of the Algerian and Tunisian experiences, aiming to assess the effectiveness of the legal frameworks in protecting digital health data.

A) Case Study: The "WannaCry" Cyberattack on the UK's National Health Service (NHS) – 2017

In May 2017, the United Kingdom's National Health Service (NHS) was the victim of a large-scale cyberattack carried out through the ransomware known as WannaCry. The malware exploited unpatched vulnerabilities in outdated Windows systems within hospitals and healthcare institutions, resulting in:

- The disruption of hundreds of medical computers, imaging devices, and digital booking systems.
- The cancellation of thousands of medical appointments and surgical procedures.
- The closure of emergency departments and redirection of patients to other facilities.

- Direct threats to patient safety due to the inaccessibility of critical medical records.

The ransomware encrypted data on infected systems and demanded payment in Bitcoin to restore access, effectively holding sensitive health data hostage.

Legal Implications :

- This attack constituted a direct violation of digital health sovereignty, as external actors gained control over nationally critical health infrastructure and data.
- It exposed significant legislative and security gaps in the protection of healthcare systems and digital assets.
- The incident prompted widespread calls for stronger cybersecurity regulations in the health sector and highlighted the need for coordinated international legal frameworks to address cross-border cybercrime, particularly against critical services such as healthcare. National Audit Office. (2018)

B) Case Study: Cyber Threats to Digital Health Sovereignty – The Tunisian Experience (2022)

In early 2022, the healthcare sector in Tunisia experienced a major cybersecurity incident that exposed vulnerabilities in the nation's digital health infrastructure. The attack targeted the digital platforms managed by the Ministry of Health, particularly those related to pandemic response coordination, including COVID-19 vaccination tracking and hospital resource management systems.

The cyber intrusion resulted in temporary disruptions in public access to vaccination records and delays in the internal coordination of medical services across hospitals. More critically,



it raised serious concerns about the exposure of personal health information belonging to thousands of citizens, thereby jeopardizing data confidentiality and institutional trust in digital health governance.

This incident illuminated the broader challenge of securing digital health sovereignty in a legal environment where dedicated regulatory instruments for health data protection were either underdeveloped or fragmented. Tunisia, like several other countries in the region, had relied primarily on general information technology legislation without a specialized legal framework tailored to the healthcare domain.

The repercussions of the attack extended beyond technical recovery; it triggered renewed national dialogue on the legal gaps surrounding cybersecurity in critical sectors. It also accelerated the development of strategic plans aiming to enhance national control over digital infrastructure, reduce dependency on foreign technology providers, and introduce sector-specific laws that prioritize the integrity and security of health data systems.

This case underlines the essential role of comprehensive legal frameworks in reinforcing digital sovereignty and the urgent need for integrated cybersecurity policies that treat health data as a matter of national security.

Chapter Two: Preventive and Remedial Mechanisms for Combating Crimes Affecting Digital Health Sovereignty under Algerian Legislation

Crimes that infringe upon digital health sovereignty represent some of the most serious challenges facing individuals in their daily lives and states in their efforts to preserve national security and sovereignty-particularly in light of rapid technological and digital transformations impacting various sectors. This digital

shift has also given rise to severe violations of individual privacy and rights, prompting lawmakers in many countries, including Algeria, to adopt strict measures to combat such offenses.

In response, a range of legal and preventive mechanisms have been implemented to strengthen cybersecurity, whether through the development of legislative frameworks or the adoption of advanced technological tools to counter these threats. This chapter will explore the legal and technical measures established within the Algerian legal system to address this growing concern.

Section One: Cybersecurity as an Imperative to Confront Threats to Digital Health Sovereignty

There is a strong interconnection between cybersecurity and digital health sovereignty. The more secure a country's health systems are, the greater its capacity to exercise full control over its digital health data and platforms.

Subsection One: Conceptual Perspectives on Cybersecurity

The concept of cybersecurity varies depending on the perspective from which it is approached:

- From a technical standpoint, cybersecurity refers to the tools, techniques, and procedures required to protect digital information from internal and external threats.
- From a legal perspective, legal scholars define cybersecurity as the set of legal measures and procedures aimed at safeguarding the confidentiality, integrity, and privacy of information content, and combating attempts to exploit digital systems to commit information-related crimes. (Ammimer&Younsi, 2020, p. 40).
- From a practical and procedural viewpoint, cybersecurity can be summarized in the following key elements:



1. It consists of defensive tools used to detect and neutralize intruders.
2. It involves protecting computer networks and the information they contain from breaches, damage, or disruption.
3. It aims to reduce malicious threats targeting software and data on computers and networks.
4. It includes all necessary tools to detect intrusions, block viruses, enforce authentication protocols, and enable encrypted communications. (Bara, 2017, p. 257).

Subsection Tow: Cybersecurity During the COVID-19 Pandemic

The healthcare sector witnessed one of the largest cyberattack waves in modern history during the year 2020, at the height of the COVID-19 pandemic. These attacks targeted vaccine supply chains and internet-connected refrigeration units belonging to Pfizer, a leading pharmaceutical company involved in COVID-19 vaccine distribution. (Ammimer&Younsi, 2020, p. 38)

Earlier, in 1997, the United Nations Commission on International Trade Law (UNCITRAL) issued a report urging states to enhance the security of information systems. Article 02-02 of the model law recognized the evidentiary value of data messages, provided that their methods of storage, transmission, and preservation are reliable. The UNCITRAL Model Law also emphasized the importance of regulating the creation, exchange, and retention of electronic data to ensure the reliability of digital transactions.

Section Two: Procedural and Preventive Mechanisms to Combat Crimes Affecting Digital Health Sovereignty

In this section, we address the preventive and procedural mechanisms adopted and institutionalized by the Algerian

legislator to combat crimes undermining digital health sovereignty, focusing on the following areas:

Subsection One: The National Authority for the Prevention of Risks Related to Digital Health Sovereignty

In recognition of the vital need to protect digital health sovereignty, the Algerian legislator, under Law No. 09/04, established the National Authority for the Prevention of Risks Related to Information and Communication Technologies. This institution is tasked with formulating strategies to enhance digital health security. It is an independent public entity with legal personality and financial autonomy, operating under the authority of the President of the Republic.

The authority comprises a Steering Council and a General Directorate, both of which are required to submit periodic activity reports, in accordance with Article 13 of Law No. 09/04. (Law No. 09-04, on the Prevention of Offenses Related to Information and Communication Technologies, Official Gazette No. 47 of 2009.)

The authority's key responsibilities include:

- Proposing preventive strategies to protect digital health sovereignty.
- Coordinating national efforts to combat cyber risks affecting public health.
- Supporting judicial and security agencies in investigating digital crimes that threaten the safety of health data, as outlined in Article 04 of Presidential Decree No. 20/183, dated July 13, 2020, on reorganizing the authority (Official Gazette No. 40, July 18, 2020).
- Monitoring electronic communications to prevent their use in threatening health security.



- Preserving and analyzing digital data within health systems for use in legal proceedings (Saad Ghaleb, 2006, p. 226).

The authority also monitors digital content related to public health to verify its accuracy and collaborates with both national and international bodies to combat digital health violations. While this legislative initiative marks significant progress, it still requires continuous development to keep pace with evolving digital threats.

Legal solutions to enhance cybersecurity and combat cybercrime include:

- Enforcing strict legislation criminalizing cyber offenses and specifying appropriate penalties.
- Conducting regular audits and inspections to ensure hospitals comply with security standards.
- Developing advanced cybersecurity technologies to prevent breaches and malicious attacks (Hadid & Karbeit, 2014, p. 202).
- Enhancing international cooperation in combating cybercrime and investigating breaches.

It is also worth noting that effective protection from cybercrime requires a collective effort between public and private sectors, as well as continuous training and awareness programs for administrators and healthcare professionals.

Subsection Two: Digital Inspection and Seizure within Health Information Systems

According to article 2, paragraph 2 of law no. 09/04, a health information system is defined as an electronic system dedicated to the automated processing of health data. (Presidential Decree No. 20-183, on the reorganization of the National Authority for the Prevention and Fight against ICT-related Offenses, Official Gazette No. 40 of 2020). To ensure the security of digital health systems, Algerian law permits several monitoring procedures, including the surveillance

of electronic communications and, when necessary, the inspection and seizure of stored data-even if accessed remotely.

If relevant digital evidence is found, it must be copied onto legally admissible electronic storage devices. When technical constraints prevent this, competent authorities are required to take measures to prevent unauthorized access to the data. Experts may be consulted to assist in these inspections and investigations, as stipulated in Article 06 of Law No. 09/04.

Subsection Three: International Cooperation in Protecting Digital Health Sovereignty

In accordance with Article 15 of Law No. 09/04, Algerian criminal courts have jurisdiction over cybercrimes that target national health institutions-even if the offenses are committed outside Algerian territory. To enhance investigative mechanisms and identify perpetrators of digital health violations, the law allows competent judicial authorities to cooperate and exchange international legal assistance in collecting digital evidence, in line with applicable treaties and the principle of reciprocity.

Section Three: Technical Mechanisms for Protecting Digital Health Sovereignty

Through Law No. 09/04 on the Prevention of Offenses Related to Information and Communication Technologies, the Algerian legislator has adopted a range of effective technical mechanisms to counter cybercrimes targeting digital health infrastructure. These mechanisms aim to enhance cybersecurity and address electronic threats by implementing modern control systems and advanced tools to protect information systems more efficiently and effectively.



Subsection One: Digital Surveillance in the Health Sector

Digital health surveillance refers to the use of advanced digital technologies to monitor and regulate health-related content, ensuring data reliability and public health safety. Although Law No. 09/04 does not explicitly define this concept, it outlines specific circumstances under which such surveillance may be conducted, including:

- Counteracting sabotage activities that threaten national health security.
- Preventing cyberattacks targeting healthcare systems or sensitive medical data.
- Supporting security investigations when traditional evidence-gathering methods are insufficient.
- Facilitating international cooperation based on mutual legal assistance agreements.

Importantly, Algerian law requires prior written judicial authorization before implementing any form of digital surveillance.

Subsection Two: The Role of Digital Service Providers in Safeguarding Digital Health Sovereignty

According to Article 02/04 of Law No. 09/04, digital service providers are entities responsible for enabling digital connectivity and processing electronic data. These providers are legally obligated to support competent authorities by:

- Recording and analyzing digital health data.
- Assisting in tracing communications relevant to the health sector.

- Deleting unlawful health content and blocking access to websites that disseminate misleading information about public health.
- Implementing technical measures to prevent unauthorized access to digital health data.
- Maintaining strict confidentiality during investigations.

As per Article 10/03 of the same law, service providers must comply with requests from authorities and ensure the protection of sensitive data.

Moreover, Article 11 stipulates the categories of data that must be made available when required, including:

- The identity of users accessing digital health services.
- Information about the devices used to connect to health platforms.
- The time and duration of each connection to digital health systems.
- Details about the services accessed and the health service providers involved.
- Logs of digital health websites visited.

Comparative Analysis: Algeria and Tunisia in Addressing Digital Health Sovereignty Threats

The rising frequency and sophistication of cyber threats targeting healthcare infrastructure have prompted several countries in the Arab region to reassess the resilience of their digital health systems. A comparative examination of Algeria and Tunisia reveals two distinct legal and strategic approaches to safeguarding digital health sovereignty.



1. Legal Framework and Institutional Readiness:

Algeria has taken an early step in addressing cyber-related offenses through the enactment of Law No. 09/04 on cybercrime, which criminalizes unauthorized access, system sabotage, and data breaches. Although the law is not specific to the health sector, it provides a general foundation for prosecuting digital offenses that impact medical platforms. Algeria has also introduced regulatory bodies such as the National Authority for the Prevention and Fight against Cybercrime, but health-sector-specific cybersecurity policies remain limited in scope and application.

In contrast, Tunisia, prior to the 2022 incident, lacked a comprehensive cybersecurity law and instead relied on fragmented ICT-related regulations. The absence of a legal instrument tailored to healthcare data protection limited the government's capacity to react effectively to targeted cyberattacks. However, the experience acted as a catalyst, prompting discussions on a national cybersecurity strategy that prioritizes critical sectors such as health and introduces frameworks for digital sovereignty.

2. Institutional Dependency and Infrastructure Resilience:

Both countries face significant challenges related to technological dependency, especially reliance on foreign-hosted platforms, imported digital health solutions, and externally managed cloud infrastructure. This undermines the autonomy of national health systems and increases vulnerability to foreign surveillance or service disruption.

Algeria's infrastructure benefits from stronger state control, particularly over national data centers, yet the integration of cybersecurity within the health system remains underdeveloped. Tunisia, though more open to private and foreign partnerships in digital health, has recognized the importance of building local

capacity and promoting data localization policies following the attack.

3. Strategic Policy Direction:

Algeria appears more focused on criminalization and prosecution through its penal framework, while Tunisia's recent shift leans toward preventive strategies, policy reform, and governance restructuring. Both approaches are essential and, if combined, could offer a more holistic model for digital health sovereignty.

This comparison highlights that while Algeria benefits from a pre-established legal base, it must modernize and health-sectorize its cybersecurity approach. Tunisia, on the other hand, is transitioning from reactive to proactive digital health governance. The convergence of both models-robust legal enforcement and comprehensive sector-specific regulation-could serve as a prototype for other Arab states navigating the complex terrain of digital health sovereignty.

Conclusion:

The increasing integration of digital technologies in the healthcare sector has undoubtedly improved the quality, speed, and accessibility of medical services. However, this digital transformation has brought with it complex and evolving threats that directly undermine digital health sovereignty-a concept that embodies the full and independent control of nations over their health-related data and digital infrastructures.

The study has shown that cybercrimes targeting health systems are no longer isolated technical incidents but constitute real threats to national sovereignty, patient safety, and institutional trust. These crimes, often transnational and technologically sophisticated, expose critical gaps in both legal and technological infrastructures.



In the Algerian context, Law No. 09/04 on cybercrime provides a foundational legal framework to criminalize digital offenses. However, it lacks sectoral specificity, particularly regarding health-related data protection and emergency response protocols in the event of cyber incidents affecting hospitals and medical platforms. Tunisia's experience in 2022 highlighted similar structural weaknesses, yet it also offered a lesson in policy adaptation and reform, showing the value of aligning cybersecurity strategy with sector-specific vulnerabilities. Addressing these challenges requires a paradigm shift—from general legal provisions to comprehensive, specialized, and adaptive legal frameworks that:

1. Recognize the healthcare sector as critical national infrastructure.
2. Mandate security-by-design principles in digital health systems.
3. Foster regional and international cooperation for cross-border threat mitigation.
4. Promote investment in cybersecurity capacity-building within public health institutions.

Protecting digital health sovereignty is no longer an option, but a legal and strategic necessity. The ability of a nation to protect its citizens' medical data and ensure the continuity of health services in cyberspace is now a benchmark of true national sovereignty in the digital age.

Recommendations for Strengthening Legal Protection of Digital Health Sovereignty:

1. Introduce a dedicated legal framework focusing on the protection of digital health data, infrastructure, and platforms, distinct from general cybercrime legislation. This law should

address specific threats to healthcare systems and outline obligations for both public and private health institutions.

2. Legally classify digital health systems and medical databases as critical infrastructure, thereby mandating a higher level of security measures and legal protection in accordance with national sovereignty imperatives.

3. Create a specialized governmental body tasked with monitoring, preventing, and responding to cyber threats in the health sector. This authority should also coordinate with other national and international cybersecurity entities.

4. Require all health facilities, both public and private, to implement certified cybersecurity measures, including periodic risk assessments, encryption protocols, and staff training on data protection and incident response.

5. Encourage or mandate that health data be stored within national borders and managed through domestically controlled infrastructure to reduce reliance on foreign cloud providers and preserve data sovereignty.

6. Develop bilateral and multilateral legal agreements focused on cybercrime investigation, digital evidence exchange, and rapid response coordination in the event of cross-border cyberattacks targeting health services.

7. Promote public education campaigns and mandatory digital security training for medical personnel to enhance their role in protecting patient data and preventing cyber breaches at the user level.

8. Ensure that cybersecurity standards are part of the legal and technical specifications when procuring medical equipment or software, especially those connected to hospital networks or patient records.



9. Implement a mechanism for periodically reviewing and updating cybersecurity-related laws and regulations to keep pace with evolving threats, emerging technologies, and international legal standards (e.g., GDPR, HIPAA).

10. Legally require all healthcare institutions to report cyber incidents to a central authority. This would enable national risk mapping, data analysis, and preventive strategy formulation.

REFERENCES:

I. Books:

- Bara, A. (2017), *Cybersecurity and Digital Evidence: Legal and Technical Approaches*, Al-Maaref Publishing, Algeria.
- Saad Ghaleb, M. (2006), *Cybercrime and Information Security*, Dar Al-Kitab Al-Jami'i, Egypt.

II. Journal Articles :

- Ammimer, M. & Younsi, A. (2020), *Cybersecurity Challenges in the Health Sector: Legal and Practical Considerations*, Al-Haqiqah Journal, Algeria, Vol. 18, No. 2, pp. 36-42.
- Boudiaf, A. (2020), *Obstacles to the Exercise of Digital Sovereignty in the Health Sector*, Journal of Legal and Political Sciences, Algeria, Vol. 21, No. 1, p. 178.
- Hadid, S. & Karbeit, R. (2014), *Cybersecurity Mechanisms in Algerian Legislation*, Journal of Law and Society, Algeria, Vol. 12, No. 3, p. 202.
- Kadri, S. & Meklekal, F. (2022), *The Legal Value of Digital Encryption in Electronic Commerce*, Journal of Legal and Economic Research, Algeria, Vol. 7, No. 1, pp. 7-8.

- Bonnaud, G. (2013), Des données personnelles médicales sur Google, danger réel numérique en santé ? *HEGEL Review*, Paris, Vol. 3, No. 3.

III. Theses :

- Khalil, A. (2017), Legal Mechanisms to Combat Cybercrime in Light of Technological Advancements, Faculty of Law, University of Algiers 1, Algeria.

IV. Internet Sources :

- National Audit Office (2018), Investigation into WannaCry cyber-attack and the NHS, detailed website: <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs> (consulted on 07/07/2025 à 19h).
- United Nations Commission on International Trade Law (1996), UNCITRAL Model Law on Electronic Commerce (adopted on June 12, 1996, and endorsed by General Assembly Resolution No. 51/162 on December 16, 1996), <https://uncitral.un.org/en/model-laws/electronic-commerce> (consulted on 07/07/2025 à 19:40).