

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

الأمن السيبراني بين التحول الرقمي والقصور التشريعي:
دراسة في الإطار القانوني الجزائري

Henen Bouhafs¹

¹ University of Aïn Témouchent, (Algeria), Faculty of Law, henen.bouhafs@univ-temouchent.edu.dz

Laboratory for Markets, Employment, Legislation, and Simulation in Maghreb Countries

Received: 15/07 /2025

Accepted: 26/10 /2025

Published: September /2025

الملخص:

يُعدّ الأمن السيبراني أحد الركائز الجوهرية لإنجاح مشاريع التحول الرقمي، نظراً لدوره الحيوي في حماية البنى التحتية الرقمية من التهديدات والهجمات الإلكترونية التي قد تُعرقّل استمرارية الخدمات وتُضعف الثقة في البيئة الرقمية، غير أن تحقيق هذا الهدف يقتضي وجود إطار قانوني وتشريعي فعّال يواكب التطورات التكنولوجية المتسارعة، ويضمن التوازن بين متطلبات التحول الرقمي وضرورات الحماية القانونية

في هذا الإطار، تسعى هذه الدراسة إلى تحليل العلاقة بين الأمن السيبراني والتحول الرقمي، مع التركيز على الإطار القانوني المنظم للأمن السيبراني في الجزائر، واستجلاء أوجه القصور التشريعي التي تحدّ من فعاليته في مواجهة التحديات الرقمية المعاصرة، كما تتناول الدراسة بالتحليل أبرز النصوص القانونية الوطنية ذات الصلة، وتقارنها بالتجارب الدولية الرائدة، بهدف اقتراح رؤية إصلاحية لتعزيز المنظومة التشريعية الجزائرية في هذا المجال.

وتخلص النتائج إلى أن الإطار القانوني الجزائري، رغم ما شهده من تطورات ملحوظة، ما يزال جزئياً ومتعدد النصوص، الأمر الذي يضعف فعالية الحماية القانونية للفضاء السيبراني، ومن ثمّ فإن تحقيق أمن سيبراني متكامل في ظل التحول الرقمي يتطلب إصلاحاً تشريعياً ومؤسسياً شاملاً، يضمن توحيد المفاهيم القانونية، وتوضيح الاختصاصات، وتعزيز القدرات الوطنية في مجال الدفاع السيبراني.

الكلمات المفتاحية: الأمن السيبراني، التحول الرقمي، القصور التشريعي، الإطار القانوني الجزائري، حماية البيانات.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

Abstract:

Cybersecurity constitutes one of the fundamental pillars for the success of digital transformation projects, given its vital role in protecting digital infrastructures from cyber threats and attacks that may disrupt service continuity and undermine trust in the digital environment. However, achieving this objective requires an effective legal and regulatory framework that keeps pace with rapid technological developments and ensures a balance between the demands of digital transformation and the necessities of legal protection.

In this context, this study seeks to analyze the relationship between cybersecurity and digital transformation, with a particular focus on the legal framework governing cybersecurity in Algeria. It aims to identify the legislative shortcomings that limit its effectiveness in addressing contemporary digital challenges. The study also examines and analyzes the main national legal texts related to the field and compares them with leading international experiences, in order to propose a reform-oriented vision to strengthen the Algerian legislative system in this domain.

The findings indicate that, despite notable progress, the Algerian legal framework remains fragmented and dispersed across multiple texts, which weakens the overall effectiveness of legal protection in cyberspace. Therefore, achieving comprehensive cybersecurity in the context of digital transformation requires a thorough legislative and institutional reform that ensures the unification of legal concepts, clarifies jurisdictions, and enhances national capabilities in the field of cyber defense.

Key words: Cybersecurity, Digital Transformation, Legislative Shortcomings, Algerian Legal Framework, Data Protection.

Introduction:

The Internet has experienced tremendous growth over recent decades, leading to a radical transformation in society, the economy, and critical infrastructure. This digital revolution, often referred to as the "cyber civilization," has profoundly changed the ways we communicate, conduct business, and access information. Today, the Internet has become an indispensable source for information exchange and a fundamental pillar of modern life. Individuals and organizations alike leverage technology to perform essential tasks across various sectors, including banking, healthcare, government, education, human resource management, smart cities, and network systems.

Advancements in information and communication technologies, coupled with the growing need for rapid access to information, have facilitated the performance of many tasks. At the same time, however, they have posed serious global security challenges. Algeria has not been immune to these cyber threats, particularly targeting its national institutions, in addition to fraud and scam crimes aimed at individuals and groups through social media platforms, which have become an integral part of daily life and continue to see increasing usage. State institutions have become targets for hackers, whether international entities or

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

individuals, due to their strategic significance, prompting authorities to intensify efforts to strengthen cybersecurity in order to confront these threats and mitigate their impact.

The importance of cybersecurity lies in maintaining the confidentiality, integrity, and availability of computer resources, whether owned by a specific organization or connected to the network of another. In a world where more than 61% of industrial and social interactions occur online, achieving high levels of security has become essential to ensure smooth, effective, and safe interactions. The key concepts that must be considered to attain this level of security include data protection, privacy preservation, reliability and availability, in addition to cybersecurity itself.

Therefore, cybersecurity has become the primary means of preventing cybercrimes and attacks by securing industrial and social interactions and ensuring their safety.

In light of the foregoing, this study is guided by the following research question:
To what extent does the Algerian legal framework keep pace with the requirements of cybersecurity protection in the context of digital transformation?

To address this question, the research adopts an inductive approach, beginning with partial observations and analyses of real-world and contemporary cases associated with digital transformation and its implications for cybersecurity. This includes the monitoring of incidents such as cyberattacks targeting critical infrastructure, data breaches, and the implementation of modern protective strategies by specific countries and institutions. Additionally, the analytical method is applied to examine these incidents and discern the nature of the relationship between digital transformation and the increasing necessity for cybersecurity.

1-Digital Transformation and Its Impact on Cybersecurity

Digital transformation represents one of the most significant aspects of change in the modern era, serving as a decisive factor in enhancing institutional performance and improving efficiency across various sectors. However, while this transformation offers substantial opportunities for growth and modernization, it has simultaneously given rise to new challenges related to cybersecurity and the protection of information in the digital environment. In this context, this section will discuss the concept and types of digital transformation within the Algerian institutional environment, and then move on to analyze the implications of this transformation on cybersecurity, highlighting the main risks and challenges that institutions face in achieving a secure and sustainable digital transformation.

1.1- Digital Transformation: Concept and Dimensions in the Algerian Institutional Environment

Digital transformation represents a pivotal step toward modernizing Algerian institutions, as it combines the adoption of modern technologies with the restructuring of work methods. This section will address the concept and types of digital transformation within the Algerian institutional environment.

1.1.1 The Concept of Digital Transformation

We are currently living in an era of accelerated digital transformation, which has become a global phenomenon asserting its strong presence across various sectors as a result of rapid technological advancements and the comprehensive digital revolution. This transformation has contributed to redefining the concepts of efficiency and effectiveness within institutions and has generated new perspectives on organizational performance. Consequently, digitalization has emerged as a strategic necessity for achieving excellence and enhancing competitiveness across different fields.

In light of this significance, this section seeks to examine the concept of digital transformation by first defining it, and then addressing its fundamental requirement as the essential pillars for its successful implementation within institutional environments.

A. Definition of Digital Transformation

Zaoui and Souissi (2020) define digital transformation as: *"a new development model that reshapes the relationships among organizations, their stakeholders, and their clients by offering new services or products"*¹.

While Oh et al. (2022) view digital transformation as: *"an extension of the Fourth Industrial Revolution (Industry 4.0) aimed at creating social change through customer-centered business model improvements"*².

Pihir et al. (2018): *"consider it a profound transformation of organizational models, processes, and capabilities to achieve strategic advantage through the use of digital technologies"*³.

Vial (2019) defines it as: *"a process that seeks to bring about fundamental changes in organizations through the integration of information, computing, and connectivity"*⁴.

Based on the review of the literature, the researchers concluded that digital transformation consists of five main dimensions:

1. Technology
2. Processes
3. People
4. Culture
5. Business Model

It can be concluded that digital transformation entails the process of converting information and leveraging modern Internet-based technologies, such as artificial intelligence and big data analytics, to enable sectors and organizations to transition to innovative business models. This transformation contributes to the development of new products and services that

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

enhance operational efficiency and expand business reach, while generating sustainable economic and social benefits that positively impact society as a whole.

B. Requirements of Digital Transformation

Digital transformation is implemented across a spectrum that includes the following requirements:

• Technical Requirements

Digital transformation relies on an integrated ecosystem of technologies, including hardware, data, storage systems, and software, all operating within advanced technological environments and high-efficiency data centers to ensure uninterrupted operations. This transformation requires maintaining high levels of service that meet the needs of the organization's employees, customers, and suppliers, through specialized teams that manage the IT infrastructure and information networks efficiently and reliably.

• Procedural Requirements

The digital transformation process requires the development of a comprehensive information security strategy that ensures data protection and quality. This involves implementing strict controls to prevent data theft, protect information privacy, and ensure secure usage. These measures are essential to guarantee the successful implementation of digital transformation.

• Human Requirements

Human resources are a fundamental element for the success of digital transformation. This involves providing qualified and well-trained personnel with advanced digital skills in information technology usage, data analysis, and effective decision-making. Additionally, human resources must possess a comprehensive understanding and a strategic vision regarding the necessity of transitioning towards digitalization⁵

1.1.2. Types of Digital Transformation

Digital transformation encompasses various sectors and fields, with each type aiming to achieve specific objectives related to efficiency, innovation, and enhancing user or customer experience in line with the requirements of the modern digital era. The most prominent types include:

1. **Government Digital Transformation:** This type focuses on improving the delivery of governmental services to citizens and streamlining administrative procedures. It is implemented through mobile applications and websites designed to facilitate access to services and enhance the user experience.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

2. Operational Digital Transformation: This type targets the improvement of internal organizational processes through the adoption of digital technologies. It involves process automation and data analytics to enhance operational efficiency and promote continuous improvement.

3. Production and Manufacturing Digital Transformation: This type involves leveraging digital technologies to optimize production processes and foster innovation in traditional industries. It includes the use of robotics, artificial intelligence, and data analytics to achieve higher efficiency and improved product quality.

4. Supply Chain Digital Transformation: This type aims to enhance supply chain management by optimizing shipping and distribution operations. It involves using tracking technologies, digital analytics, and electronic communication to increase efficiency and collaboration with suppliers.

5. Financial Sector Digital Transformation: This type seeks to improve financial services and facilitate banking operations. It includes mobile banking applications, digital wallets, and electronic payment technologies to provide a seamless and innovative financial experience.

6. Educational Digital Transformation: This type focuses on enhancing the learning experience through the integration of digital technologies in educational methods. It encompasses e-learning platforms, online educational applications, and the provision of modern digital learning content.

7. Tourism and Hospitality Digital Transformation: This type aims to improve the experience of tourists and travelers by streamlining booking and accommodation processes. It involves the use of augmented reality technologies and digital tourism applications to enhance convenience and engagement with visitors.

8. Marketing and Sales Digital Transformation: This type relies on digital tools to strengthen marketing and sales strategies. It includes email marketing, social media engagement, and e-commerce platforms to better meet customer needs.

9. Customer Experience Digital Transformation: This type focuses on enhancing customer interactions with products and services by providing a personalized and superior experience. It leverages data analytics and artificial intelligence to accurately and effectively meet customer expectations⁶.

1.2- Implications of Digital Transformation on Cybersecurity

Digital transformation is a pivotal phenomenon that is reshaping various aspects of economic and social life. However, it has also generated increasing challenges related to protecting data and information systems from growing cyber threats. As reliance on modern technologies such as cloud computing, the Internet of Things, and artificial intelligence

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

expands, cybersecurity has become a fundamental pillar for ensuring the sustainability of this transformation and safeguarding its achievements. Accordingly, this study will address the concept of cybersecurity and highlight the major cyber challenges faced by individuals and institutions in the context of rapid digital transformation.

1.2.1. The Concept of Cybersecurity

Cybersecurity is considered one of the fundamental pillars of the digital age, as it encompasses the protection of systems and information from the growing electronic threats. In this context, I will address the concept of cybersecurity in greater depth, while discussing the dialectical relationship between digital transformation and cybersecurity requirements in the contemporary digital environment.

A. Definition of Cybersecurity

The term “Cyber” originates from the Greek word “Kybernets”, which means “helmsman” or “the one who steers the ship.” This concept was later adopted in the mid-20th century by the American mathematician Norbert Wiener, who used it to describe the idea of automatic control. Wiener defined cybernetics as “the science of control and communication in animals and machines,” explaining that it deals with the transmission of messages and information between humans and machines, or between machines themselves. From this foundation, the concept of cybernetics evolved to refer to automated processes and the interactive relationships between electronic systems and humans⁷.

Cybersecurity is: “the practice of protecting computers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also referred to as the security of networks, information systems, data, and internet-connected devices. Accordingly, it represents the field concerned with the measures and standards of protection that must be implemented or adhered to in order to confront threats, prevent attacks, or at least mitigate their impacts”⁸.

data for actors within cyberspace.”⁹

The American Institute of Certified Public Accountants (AICPA) defined cybersecurity as: “a set of practices and procedures designed to protect data and information from cyber threats”¹⁰.

The American Institute of Certified Public Accountants (AICPA) has established a comprehensive set of cybersecurity standards for the accounting profession, including the Statements on Standards for Accounting and Review Services (SSARS) and the Trust Services Principles and Review Services. These frameworks are intended to assist accountants in safeguarding the digital business environment through the implementation of effective data security and privacy controls, thereby reinforcing confidence in the systems and processes underpinning the delivery of professional services¹¹. Conversely, the National Institute of Standards and Technology (NIST, 2024) has adopted

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

the Cybersecurity Framework (CSF 2.0) as a key international reference for the development of protection strategies and the management of risks at the institutional level¹².

Cybersecurity can be defined as a set of measures and technologies aimed at protecting the digital space and computer systems from various cyber threats, such as hacking attempts and intrusions targeting networks and electronic systems. Its primary goal is to ensure the security and continuity of the information society by preventing unauthorized access to data and countering any disruptions or attacks that may affect the efficiency of computer networks. It also involves detecting viruses and malicious software that hinder electronic systems, as well as combating attempts to hack personal accounts or sabotage computer program databases.

B.The Dialectical Relationship Between Digital Transformation and Cybersecurity

The relationship between digital transformation and cybersecurity is a dialectical one based on interaction and mutual influence. The more digital transformation pathways expand, the greater the likelihood of cyberattacks and intrusions, making cybersecurity an indispensable structural element for protecting the digital space.

One of the United Nations Development Programme (UNDP) documents indicates that national digital policies should adopt a comprehensive approach that integrates cybersecurity and data protection within the regulatory framework of digital transformation, considering them as fundamental pillars of any effective digital policy¹³.

Another UNDP document titled “Inclusive by Design” highlights that digital transformation, although a driver of growth and innovation, may generate new risks related to loss of transparency, weak regulation, and increasing threats associated with cybersecurity and digital privacy. This necessitates integrating cyber protection into all stages of planning and implementation¹⁴.

In the same context, the UNDP Digital Standards document emphasizes the principle of “Do No Harm” and stresses the importance of managing data responsibly and with awareness of potential risks, including cyber threats. This highlights the ethical dimension of cybersecurity within the process of digital transformation¹⁵.

Accordingly, it becomes clear that cybersecurity is not merely a technical means of protection, but rather a strategic and ethical foundation for achieving a safe, sustainable, and inclusive digital transformation.

1.2.2. The Main Cyber Challenges in the Era of Digital Transformation

In the digital era, cybersecurity has become a critical issue affecting individuals, corporations, and governments alike. With the rapid expansion of technology and digital

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

devices, the need to protect electronic systems, networks, and data from unauthorized access, theft, and damage is more urgent than ever.

As technology continues to evolve, the efforts to safeguard organizations, employees, and critical assets from cyber threats face numerous complex challenges.

This section discusses the key challenges confronting the cybersecurity industry and explores future directions that may help address these challenges effectively.

A. The Sophisticated Nature of Cyberattacks

The increasing complexity of cyberattacks aimed at gaining unauthorized access to computer systems and networks presents a major challenge in the field of cybersecurity¹⁶. Attackers (or cyber intruders) continuously develop and employ highly advanced and sophisticated techniques to exploit system vulnerabilities and bypass security defenses.

Some of the most complex types of cyberattacks that use advanced methods to breach systems include multi-vector attacks, polymorphic and fileless malware, zero-day exploits, and advanced persistent threats (APTs).

Advanced Persistent Threats (APTs) are sophisticated, targeted, and well-organized attacks that specifically focus on sensitive sectors such as diplomacy, information technology, the military, and the chemical industry. Their goal is to extract confidential information and damage the targeted organization or sector by maintaining long-term unauthorized access through various means. APTs are often state-sponsored attacks conducted by governments or organized criminal groups to gain economic, political, or strategic advantages by stealing critical information and resources from vital infrastructures such as national defense, government agencies, manufacturing industries, and other high-value targets.

One well-known example of such an attack is Operation Aurora, a highly sophisticated cyberattack that occurred in 2009. It targeted several major technology companies including Google, Adobe, and Juniper Networks, among others. The attack used complex techniques to steal intellectual property and infiltrate the internal networks of these organizations¹⁷.

B. Internet of Things (IoT) Security

The Internet of Things (IoT) represents an emerging technology that connects billions of devices to the internet for data and information exchange. Despite its numerous advantages, it poses serious cybersecurity challenges due to multiple security vulnerabilities.

The main challenges include:

- * **Device Vulnerability:** IoT devices are often designed with limited processing power and minimal security features, making them highly susceptible to hacking and exploitation.

- * **Privacy Violations:** These devices collect vast amounts of sensitive data, which can be misused if encryption is weak or data management practices are poor.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

* Wireless Network Security: Most IoT devices rely on communication protocols such as Wi-Fi and Bluetooth, which makes them vulnerable to eavesdropping, data interception, or manipulation.

C. Cloud Computing

With the rapid expansion of cloud computing services, a range of security challenges has emerged, threatening the confidentiality of data and the integrity of digital systems. The most prominent challenges include:

* Data breaches and privacy violations resulting from storing sensitive information in external environments.

* Unauthorized access by malicious actors exploiting vulnerabilities in protection systems.

* Insecure Application Programming Interfaces (APIs) that may allow attackers to access data or manipulate services.

* Shared infrastructure, which increases the likelihood of exploiting vulnerabilities to compromise data belonging to other organizations on the same platform.

The growing reliance of organizations on cloud computing offers great flexibility and operational efficiency; however, it also exposes them to risks such as data loss, service disruption, and difficulty in managing security within multi-tenant environments. Therefore, strengthening security strategies and digital governance has become essential to ensure the safety and sustainability of cloud-based systems.

D. AI-Driven Attacks

The rapid advancement of Artificial Intelligence (AI) and Machine Learning (ML) technologies has led to the emergence of a new generation of advanced cyberattacks enhanced by AI, characterized by their high level of complexity and adaptability to defensive systems.

These attacks can be divided into two main types:

1. AI-Assisted Attacks – where attackers use AI algorithms to plan attacks, analyze systems, and identify the most effective exploitation techniques.

2. Autonomous AI Attacks – where intelligent systems carry out attacks entirely on their own, without any human intervention, leveraging their ability to learn and adapt to different environments.

The most prominent threats associated with AI-driven attacks include:

* Deepfake Attacks: These involve the creation of highly realistic fake images, videos, or audio recordings used to deceive individuals or security systems.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

* Botnet Attacks: Large networks of compromised devices controlled by AI are used to conduct large-scale operations such as Distributed Denial-of-Service (DDoS) attacks or data theft.

* Reinforcement Learning-Based Attacks: In these cases, malicious systems learn from their environment and continuously refine their attack strategies, making them more capable of exploiting vulnerabilities with increasing speed, precision, and efficiency.

2- Legislative Gaps in Cybersecurity Protection within the Algerian Legal Framework

This section will address the national legal framework for cybersecurity in Algeria, focusing on the main legislative texts governing it, and will also discuss the legislative shortcomings that limit the effectiveness of this framework in confronting the growing cybersecurity challenges.

2.1- The Legal Framework Regulating Cybersecurity in Algeria

This section will address the legal framework for cybersecurity in Algeria by examining both its legislative and institutional aspects, with the aim of highlighting the legal and regulatory foundations adopted by the state to protect cyberspace and strengthen information security at both the national and institutional levels.

2.1.1. Legislative Aspect

An analysis of the legal framework issued by the Algerian legislator in the field of cybersecurity reveals the adoption of a gradual and evolving approach to addressing this issue, through a set of legal instruments consisting of:

A. Law No. 15-04 of November 10, 2004, amending and supplementing the Penal Code

The Algerian legislator criminalized acts that infringe upon computer systems and networks in the Penal Code under Law No. 15-04¹⁸, entitled “Offenses against Automated Data Processing Systems.” This seventh section includes six articles, from Article 394 bis to Article 394 bis 6, and is considered the first law addressing cybercrime in Algeria.

B. The Preventive Law No. 04-09 of August 5, 2009, establishing specific rules for the prevention and combating of crimes related to information and communication technologies

The Algerian legislator defined the purpose of this law in Article which states that its: *“objective is to establish specific rules for the prevention and combating of crimes related to information and communication technologies”¹⁹*. It is noted that the legislator clearly determined the nature of this law by replacing the term “Offenses against Automated Data Processing Systems” with the term “Crimes related to Information and Communication Technologies,” considering both expressions synonymous with the concept of cybercrime as it is legally recognized.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

Article 2 of the law addresses the definition of these cybercrimes, encompassing information systems, digital data, data service providers, traffic data, as well as electronic communications. This reflects the comprehensive legal approach adopted by the legislator in this field.

Chapter III of the same law, entitled “Monitoring of Electronic Communications,” sets out the conditions and circumstances that justify the use of electronic surveillance. Article 4 stipulates that this measure is adopted as a preventive tool aimed at combating terrorist acts and offenses that threaten state security, in addition to protecting individuals’ privacy, thereby ensuring a balance between the requirements of public security and respect for individual rights and freedoms.

Chapter I of this law, entitled “Procedural Rules and the Inspection of Information Systems,” provides a detailed outline of the legal procedures that judicial police officers must follow when dealing with cybercrimes. The legislator clarified the methods for conducting search operations and accessing electronic storage systems and the accounts of suspects when such data are located within the national territory. However, when the information is located outside the country’s borders, the law requires recourse to the competent foreign authorities in accordance with the relevant international conventions.

Articles 5 and 6 provide for the possibility of seizing or copying electronic data to be used as evidence against the accused. Article 7 stipulates a prohibition on accessing offenders’ data when their seizure or duplication is not possible. Article 8 grants the competent authorities the power to block access to data containing criminal electronic content. Meanwhile, Article 9 emphasizes that seized data may only be used within the limits required by legal necessity, ensuring the protection of privacy and adherence to the principles of procedural justice.

Chapter IV of the law is devoted to the provisions concerning the obligations of service providers and their assistance to the competent authorities. Article 10 stipulates the obligation of telecommunications service providers to cooperate with judicial and security authorities by collecting and recording data related to the content of communications in real time, while maintaining the confidentiality of information under penalty of legal liability and sanctions.

Article 11 further specifies the procedures for preserving data related to communication traffic, including the time and duration of the communication, the type of services requested, the identification of the sender and recipient, and the websites accessed. The article also allows for the determination of the source and location of the communication when required for investigation purposes.

In addition, the law provides for severe penalties for those who violate or obstruct judicial investigations, including financial fines and imprisonment for up to five years. It also obliges internet service providers to immediately intervene to delete or block criminal digital content, and to prevent access to servers or networks containing data that violate the law.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

The key provision established by this law in Title V, the penultimate section, is the creation of a National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, as stipulated in Article 13. Article 14 defines its main missions, which include:

- * Promoting and coordinating activities aimed at preventing cybercrimes.
- * Assisting the competent authorities in investigations, information gathering, and conducting judicial expertise.
- * Exchanging information with foreign counterparts to collect the necessary data for identifying cybercriminals.

Title VI, the final section of the law, is devoted to international cooperation in the prevention and combating of cybercrime. Article 15 grants the Algerian authorities the right to prosecute cybercrimes committed outside the national territory when such offenses target state institutions or national defense. Article 16 provides for the possibility of mutual legal assistance in gathering evidence related to cybercrimes, while Articles 17 and 18 outline the mechanisms for information exchange and the adoption of precautionary measures, with restrictions on the execution of assistance requests that may infringe upon national sovereignty.

The provisions further emphasize the need to maintain strict confidentiality during the exchange of information, reflecting the Algerian legislator's commitment to strengthening international cooperation while safeguarding national interests and sovereignty. This legal framework remains a fundamental reference for addressing cybercrime in Algeria to this day.

C.Ordinance No. 11-21of 16 Muharram 1443, corresponding to August 25, 2021, concerning the establishment of the National Judicial Pole specialized in combating cybercrime:

In order to reinforce the previously mentioned substantive, procedural, and preventive laws, the Algerian legislator amended Book One of Ordinance No. 155-66²⁰ of 1966 by adding a Sixth Title entitled "The National Judicial Pole for Combating Crimes Related to Information and Communication Technologies." This new section includes Articles 211 bis 22 to 211 bis 29.

.2.1.2 Institutional Aspect

Algeria has a significant number of institutions and branches affiliated with national bodies related to the field of cybersecurity. These entities can be classified into two main categories:

A. Administrative Bodies Responsible for Cybersecurity

***The National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies:**

This authority was established in 2009 under Article 13 of Decree No. 04-09and placed under the direct supervision of the Minister of Justice, Keeper of the Seals. However, it did not become operational until the issuance of Presidential Decree No. 15-261 of 2015.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

The authority is entrusted with the mission of proposing the key elements of the national strategy for the prevention and combating of crimes related to information and communication technologies, as well as assisting judicial authorities and law enforcement agencies in addressing such crimes through the collection, analysis, and provision of specialized judicial expertise.

It also plays a vital role in the preventive monitoring of electronic communications to detect crimes linked to terrorism, sabotage, or threats to state security. In addition, the authority is responsible for cooperation, coordination, training, and the exchange of expertise with various national and international bodies within its area of competence, thereby strengthening national efforts to protect cyberspace and combat cybercrime²¹.

*** The Information Systems Security Agency**

This administrative institution was established in 2020 to carry out broad responsibilities in the field of developing, coordinating, and implementing the components of the National Strategy for Information Systems Security. Its duties also include conducting digital investigations in cases of cyberattacks or incidents, as well as certifying and approving information systems security products, with the aim of strengthening the state's level of digital protection and readiness and keeping pace with the rapid developments in the field of cybersecurity.

*** The National Council for Information Systems Security**

This body was established in 2020 and represents the cornerstone of the national cybersecurity framework. It is chaired by the Minister of National Defense and includes representatives from seven key government ministries, reflecting the strategic nature of its mission and its importance in safeguarding the country's digital space.

The Council is closely linked to the National Agency for Information Systems Security, as it is responsible for reviewing the elements of the National Strategy for Information Systems Security proposed by the agency, approving its action plan, and examining and endorsing its activity reports. It also holds the authority to review any draft legislative or regulatory text related to information systems security, thereby ensuring a unified vision and coordinated national efforts in the field of cybersecurity²².

B. Operational Bodies in the Field of Cybersecurity

***The Center for the Prevention of Computer and Cybercrime**

The Center for the Prevention of Computer and Cybercrime operating under the authority of the National Gendarmerie Command, is one of the leading security institutions specialized in combating cybercrime. It was established in 2008 with the aim of **supporting other security agencies and cooperating with judicial authorities to counter various forms of digital crime.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

The center focuses on developing modern technical and investigative methods to address this type of crime and has played a pivotal role in uncovering and handling numerous cases related to electronic threats, as well as cyberattacks and hacking operations targeting security, communications, and sensitive government systems. As such, it has become one of the key pillars of Algeria's national cyber defense framework.

The National Institute of Forensic Science and Criminology

This institute is considered one of the most prominent and highly specialized institutions in combating crime in all its forms. It is distinguished by its reliance on modern scientific approaches within the field of criminal justice, which has enabled it to integrate academic knowledge with practical security applications²³.

Its mastery of advanced technological tools has significantly strengthened its ability to confront new and constantly evolving forms of crime, particularly those based on emerging technologies. The institute also deals with cases related to transnational organized crime, networks threatening national security, and cyberterrorism, among other contemporary challenges.

In this regard, the National Gendarmerie Command successfully handled more than 4,600 cybercrime cases in 2022, reflecting the institution's growing effectiveness in combating digital crime and reinforcing national security.

***The Central Directorate for Combating Cybercrime of the National Police**

The Central Directorate for Combating Cybercrime of the National Police is one of the most prominent specialized institutions established in response to the rapid transformations of cyberspace. In 2011, the General Directorate of National Security created the first specialized unit in this field, which was later expanded to all 48 provinces in 2013. With the growing risks and networks of cybercrime, a Central Directorate was established in 2015 within the Judicial Police Department, becoming the national reference authority in the fight against this type of crime.

This directorate has handled a large number of both domestic and international complaints, successfully investigating cases affecting the privacy of individuals and institutions, as well as cyberterrorism, transnational criminal networks, and crimes involving the online exploitation of children.

It is worth noting that the first international case handled by the Algerian police dates back to 2009, and involved the hacking of banking data following a report from the U.S. Federal Bureau of Investigation (FBI). This early experience helped establish Algeria's reputation as a leading actor in combating cybercrime, thanks to the high competence of its personnel and its advanced technological capabilities.

Today, Algeria plays an active role in international training programs and the exchange of expertise, and is a key member in global efforts to combat transcontinental

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

cybercrime, through close cooperation with both the International Criminal Police Organization (INTERPOL) and the African Union Mechanism for Police Cooperation (AFRIPOL).

2.2- Shortcomings in the Legal Framework for Cybersecurity

Despite the existence of legislation and regulations related to cybersecurity, several shortcomings hinder the achievement of effective protection, including:

A. Legislative Gaps:

- * The existing laws are insufficient to address modern digital crimes, such as AI-driven attacks or advanced persistent threats (APTs).

- * Legal loopholes make it difficult to impose appropriate penalties on offenders.

B. Organizational and Procedural Deficiencies:

- * Weak monitoring and oversight mechanisms for digital institutions and government services.

- * Lack of clear procedures to ensure the effective implementation of cybersecurity laws in practice.

C. Insufficient Protection of Data and Infrastructure:

- * Absence of comprehensive legislation that fully protects personal data and sensitive information.

- * Ongoing challenges in securing digital infrastructure against continuous and sophisticated cyberattacks.

From this analysis, it appears that Algeria needs a comprehensive development of its legal and regulatory framework to make it more effective in safeguarding cybersecurity. This includes updating legislation, strengthening oversight mechanisms, and adopting international best practices in the field.

Conclusion:

In light of the foregoing, this research paper concludes that there is an urgent need to prioritize cybersecurity for both individuals and the state, particularly in the era of artificial intelligence, as it serves as a key tool for addressing cyber challenges and electronic crimes. Despite the efforts made by Algeria through its criminal policies, whether via traditional laws or specialized provisions, these measures remain insufficient to establish a comprehensive criminal policy aligned with the digital transformation.

Therefore, it is essential to undertake additional efforts that correspond with this transformation, taking into account Algeria's strategic position, the scale of threats it faces, and its capacity to withstand risks by improving and strengthening the cybersecurity

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

environment. In this context, a number of key recommendations can be formulated to enhance the response to threats and protect the national digital infrastructure :

1. Updating the National Legislative Framework

- * Review traditional criminal laws to encompass modern cybercrimes.
- * Enact specific cybersecurity legislation addressing emerging digital threats such as artificial intelligence, the Internet of Things, and attacks on critical infrastructure.

2. Joining International Agreements

- * Ratify the Budapest Convention of 2001 on cybercrime and enhance international cooperation in this field.
- * Participate in regional and international networks to combat cross-border cybercrime.

3. Strengthening National Institutional Capacities

- * Establish specialized cybersecurity units within governmental and private institutions.
- * Develop ongoing training programs for legal and technical personnel to effectively address cyber threats.

4. Enhancing Digital Oversight and Regulation

- * Implement clear mechanisms to monitor cyber threats and protect personal and institutional data.
- * Encourage institutions to adopt international information security standards, such as ISO 27001.

5. Community Awareness and Education

- * Launch awareness campaigns to educate individuals about cyber risks and preventive measures.
- * Integrate educational programs in schools and universities to promote digital literacy and cybersecurity awareness.

6. Promoting Scientific and Technological Research

- * Support applied research and studies in cybersecurity and emerging technologies.
- * Encourage collaboration between universities, the private sector, and the government to develop innovative solutions for combating digital crimes.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

References:

- 1- F. Zaoui and N. Souissi, "Roadmap for Digital Transformation: A Literature Review," *Procedia Computer Science*, vol. 175, 2020.
- 2- K. Oh, H. Kho, Y. Choi, and S. Lee, "Determinants for Successful Digital Transformation," *Sustainability*, vol. 14, no. 3.
- 3-I. Pihir, K. Tomićić-Pupek, and M. T. Furjan, "Digital Transformation Insights and Trends," *Central European Conference on Information and Intelligent Systems*, 2018.
- 4-G. Vial, "Understanding Digital Transformation: A Review and a Research Agenda," *Journal of Strategic Information Systems Review*, vol. 28, no. 2, 2019.
- 5- Walid Kamel Allam, "Digital Transformation and Its Impact on Enhancing the Competitive Advantage of Banking Services from the Perspective of Customer Service Officers: A Field Study Applied to the Banking Sector in Upper Egypt," *The Scientific Journal of Economics and Commerce*, Issue 52, 2022.
- 6- Omar Mohammedi, Financial Inclusion through Electronic Payment: An Analytical Study of the Algerian Experience, *Arab Journal of Financial and Banking Sciences*, Vol. 2, No. 9, 2021.
- 7- Ben Merzoug, Antar. "The Electronic Dimension of Algerian Security Policy in Combating Terrorism." *Journal of Human and Social Sciences*, No. 38, 2018.
- 8 -Jabbour Al-Ashqar, Mona. "Cybernetics: The Obsession of the Era."Arab Center for Legal and Judicial Research, Beirut, 2017.
- 9- Bougrara, Y. *Cybersecurity: The Algerian strategy for security and defense in cyberspace*. African and Nile Basin Studies Journal, (3), Democratic Center, Berlin, 2018
- 10- Daoud, M. M., & Serag, A. A. *A proposed framework for studying the impact of cybersecurity on accounting information to increase trust in the financial reports in the context of Industry 4.0: An event, impact and response approach*. *Trade and Finance*, 42(1), 2022.
- 11- Through these standards, the American Institute of Certified Public Accountants (AICPA) seeks to assist organizations in protecting their data and ensuring business continuity. These standards include:
 1. Risk Assessment: Identifying potential threats and evaluating the risks associated with systems and data.
 2. Access Control:Regulating who can access sensitive information and how it is used.

Cybersecurity Between Digital Transformation And Legislative Shortcomings: An Analytical Study Of The Algerian Legal Framework

Bouhafs Henen

3. Encryption: Applying cryptographic methods to safeguard data during storage and transmission.

4. Awareness and Training: Educating employees on cybersecurity best practices and how to recognize potential attacks.

5. Incident Response: Establishing plans for a rapid and effective response in the event of a security breach.

12 -NIST. *Fiscal Year 2024 Annual Report on Cybersecurity and Privacy Program (SP 800-236)*. National Institute of Standards and Technology. Retrieved from:

<https://www.nist.gov/publications/fiscal-year-2024-annual-report-nist-cybersecurity-and-privacy-program>, 2024.

13- United Nations Development Programme (UNDP). *Digital Transformation Framework – Whole-of-Society*. New York: United Nations Development Programme, 2021.

Available at: <https://gobiernu.cw/wp-content/uploads/2021/09/UNDP-Whole-of-Society-Digital-Transformation.pdf>

14- United Nations Development Programme (UNDP). *Inclusive by Design: Accelerating Digital Transformation for the Global Goals.** New York: United Nations Development Programme, 2022.

Available at: <https://digitalstrategy.undp.org>

15- United Nations Development Programme (UNDP). *UNDP Digital Standards*. New York: United Nations Development Programme, n.d.

Available at: <https://www.undp.org/digital/standards>

16- Tankard, C., *Advanced persistent threats and how to monitor and deter them*, Network Security, (8), 16–19, 2011, doi:10.1016/S1353-4858(11)70086-1.

17 -Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro, *Cyber Security: State of the Art, Challenges and Future Directions*, Department of Information Technology, Vol. 2, 2024, p. 04.

18- Law No. 04-15 of 10 November 2004, amending the Penal Code, published in the Official Gazette No. 71 of 2004.

**Cybersecurity Between Digital Transformation And Legislative Shortcomings:
An Analytical Study Of The Algerian Legal Framework**

Bouhafs Henen

19- Law No. 04-09 of 5 August 2009, concerning specific rules for the prevention and combating of crimes related to information and communication technologies, published in the Official Gazette No. 47 of 16 August 2009

20- Ordinance No. 156-66 of 8 June 1966, containing the Penal Code as amended and supplemented, published in the Official Gazette No. 49 of 11 June 1966.

21- Presidential Decree No. 261-15 of 24 Dhu al-Hijjah 1436, corresponding to 8 October 2015, defining the composition, organization, and operating procedures of the National Body for the Prevention and Combating of Crimes Related to Information and Communication Technologies.

22- Presidential Decree No. 05-20 of 24 Jumada al-Awwal 1441, corresponding to 20 January 2020, concerning the establishment of a national system for information systems security.

23- Rabah Souad, “*Regulations for Combating Cybercrime*,” Journal of Algerian and Comparative Public Law, No. 1, June 2021.