

Cybersecurity in the Age of Artificial Intelligence and Big Data: A Critical Analysis of Security and Ethical Challenges under National and International Legal Frameworks



Tassadit NEBBAD^{1*}

University of Mouloud MAMMERI -Tizi Ouzou-, Algeria¹

Submission date: 05/01/2026 Acceptance date: 22/02/2026 Publication date: 30/06/2026



Abstract:

The contemporary global landscape is experiencing a profound digital transformation, driven by the increasing deployment of artificial intelligence and big data, thereby generating extensive opportunities for technological innovation and socio-economic development. Simultaneously, this transformation has exposed vulnerabilities within information systems and exacerbated threats to both individual privacy and national security, thereby positioning cybersecurity as a strategic imperative to reconcile the free flow of data with robust digital safeguards. The significance of cybersecurity is further amplified by the dual use potential of artificial intelligence and the strategic utility of big data. Accordingly, examining the impact of these technologies on cybersecurity necessitates an integrated legal and analytical methodology, encompassing both theoretical underpinnings and national as well as international regulatory frameworks.

Key Words: Cyber security; Big Data; Artificial Intelligence; Digital Transformation; Automated Processing.

الأمن السيبراني في عصر الذكاء الاصطناعي والبيانات الضخمة: دراسة تحليلية للتحديات الأمنية والأخلاقية على ضوء التشريعات الوطنية والدولية

ملخص: يشهد العالم اليوم تحولاً رقمياً عميقاً بفعل زيادة الاعتماد على الذكاء الاصطناعي والبيانات الضخمة، مما أتاح فرصاً واسعة للنمو والابتكار، لكنه كشف في المقابل عن هشاشة البنى المعلوماتية وتزايد التهديدات التي تمس خصوصية الأفراد وأمن الدول، مما جعل من الأمن السيبراني عنصراً استراتيجياً يهدف إلى تحقيق التوازن بين حرية تدفق المعلومات والحماية من المخاطر الرقمية، خاصة مع الاستخدام المزدوج للذكاء الاصطناعي الذي يمكن أن يدعم الدفاع أو يُستغل للهجمات المتطورة، وتحول البيانات الضخمة إلى ثروة رقمية محورية تستوجب حماية مضاعفة. وبناءً على ذلك، تبرز أهمية دراسة تأثير هذه التقنيات على منظومة الأمن السيبراني من منظور قانوني وتحليلي شامل، ضمن إطار بحثي يتناول الأسس النظرية أولاً ثم الإطارين القانوني الوطني والدولي ثانياً.

الكلمات المفتاحية: الأمن السيبراني، البيانات الضخمة، الذكاء الاصطناعي، التحول الرقمي، المعالجة الآلية للمعطيات.

Cyber sécurité à l'ère de l'intelligence artificielle et des méga données : étude analytique des défis sécuritaires et éthiques au regard des législations nationales et internationales

Résumé :

Le contexte mondial connaît aujourd'hui une transformation numérique profonde, résultant de l'essor du recours à l'intelligence artificielle et aux méga données, laquelle a ouvert de vastes perspectives de croissance et d'innovation. Toutefois, cette évolution a simultanément mis en évidence la fragilité des infrastructures informationnelles ainsi que l'intensification des menaces portant atteinte à la vie privée des individus et à la sécurité des États.

Dans ce cadre, la cyber sécurité s'impose comme un enjeu stratégique visant à établir un équilibre entre la liberté de circulation de l'information et la protection contre les risques numériques, notamment face à l'usage dual de l'intelligence artificielle, susceptible de renforcer les mécanismes de défense ou d'être exploitée à des fins d'attaques sophistiquées, ainsi qu'à la transformation des méga données en une richesse numérique centrale nécessitant une protection renforcée.

L'étude de l'impact de ces technologies sur le système de la cyber sécurité revêt une importance particulière dans une approche juridique et analytique globale, s'inscrivant dans un cadre de recherche qui aborde, en premier lieu, les fondements théoriques, puis, en second lieu, les cadres juridiques national et international.

Mots Clés: Cyber sécurité, méga données, intelligence artificielle, la transformation numérique, le traitement automatique des données.

Introduction:

The contemporary world is experiencing a profound and unparalleled transformation, driven by the digital revolution and propelled by artificial intelligence and big data, which have emerged as the principal catalysts of digital transformation across economic, social, and technological domains. This evolution has created extensive opportunities for innovation and growth; yet, it has concurrently exposed vulnerabilities within information infrastructures and posed significant challenges to state security and digital sovereignty, while simultaneously endangering individual privacy and the right to personal data protection.

In this context, cybersecurity has emerged as a strategic, multidimensional concept encompassing technical, legal, and ethical dimensions, aiming to reconcile the free flow of information with protection against digital threats. This challenge has been exacerbated by the growing utilization of artificial intelligence, which functions as a dual-impact factor in cybersecurity: it can enhance early detection and response capabilities against cyber-attacks, yet it may also be exploited to develop offensive tools with self-learning capabilities and advanced concealment techniques.

Regarding big data, it has emerged as the digital asset of the modern era, rendering it a prime target for cyber-attacks and a fertile ground for the illicit exploitation of sensitive information.

Accordingly, addressing cybersecurity in the context of artificial intelligence and big data technologies requires a comprehensive legal and analytical perspective, aimed at balancing the imperatives of technological advancement with the demands of legislative and ethical regulation. Within this framework, the central question arises: **To what extent do advancements in artificial intelligence and big data technologies impact the cybersecurity system?**

To address this question, this research paper is organized into two principal sections: the first explores the theoretical framework of cybersecurity in the context of artificial intelligence and big data, while the second analyzes national and international legal systems governing cybersecurity in light of advancements in artificial intelligence and the expanding availability of extensive data repositories.

THE FIRST TOPIC:

THE THEORETICAL FRAMEWORK OF CYBERSECURITY IN THE ERA OF ARTIFICIAL INTELLIGENCE AND BIG DATA

Cybersecurity in the digital age constitutes one of the major strategic issues that increasingly draw the attention of states, institutions, and individuals alike, given its role as a fundamental element in safeguarding cyberspace and protecting information infrastructures from the growing threats accompanying rapid technological advancement. The greater the reliance on digital technologies across various fields of life, the more urgent the need becomes to develop effective mechanisms that ensure information security and the integrity of digital systems against intrusion and misuse.

In parallel, artificial intelligence and big data have emerged as two central pillars of the modern digital system, forming a relationship of complementarity and mutual interaction with cybersecurity. Artificial intelligence significantly contributes to strengthening cybersecurity capabilities by developing systems capable of learning and early detection of attacks, while big data provides an extensive knowledge base used to analyze patterns and extract risk indicators. However, this very development opens the door to new challenges, manifested in the emergence of advanced forms of cyber-attacks that employ artificial intelligence techniques themselves to conceal their traces or circumvent traditional protection mechanisms.

Accordingly, this topic examines the conceptual framework of cybersecurity and its relationship with artificial intelligence and big data by outlining the fundamental concepts (**first requirement**). It then analyzes the dual impact of artificial intelligence on cybersecurity, as both a supporting tool and a potential source of threats (**second requirement**).

First requirement: A Conceptual Introduction to cybersecurity in the Era of Artificial Intelligence and Big Data

This conceptual introduction constitutes a foundational basis for comprehending the theoretical framework connecting cybersecurity, artificial intelligence, and big data as interrelated and mutually reinforcing constructs that shape the modern digital environment. The rapid advancement of information technology has created a new reality wherein the protection of cyberspace constitutes an essential requirement, artificial intelligence functions as a primary instrument for developing security systems and conducting risk analyses, and big data serves as the foundational resource supporting diverse intelligent applications.

From this vantage point, this section seeks to elucidate the fundamental concepts of cybersecurity (**first section**), artificial intelligence (**second section**), and big data (**third section**), in order to define their precise meanings and emphasize the

interconnections among them, thereby establishing the foundation for comprehending their mutual influence within the contemporary digital security framework.

First section: The Concept of cybersecurity

Cybersecurity constitutes a critical domain, as cyber-attacks pose threats to individuals, institutions, and states. The exponential growth of the Internet has generated a complex environment necessitating the safeguarding of sensitive data and critical infrastructure.¹ To delineate the concept of cybersecurity with precision, it is essential to provide its definition and outline its foundational principles. To clarify the concept of cyber security with precision, it is necessary to present its definition (**first**) and outline its importance (**second**).

First: definition of cybersecurity

The International Telecommunication Union (ITU) defines cybersecurity as a discipline focused on safeguarding the digital space, including its associated information systems and digital assets, through a comprehensive set of policies, procedures, and technologies designed to mitigate threats and risks. This includes the protection of devices, infrastructure, applications, services, and data transmitted or stored within networks, with the aim of ensuring their integrity and continuity, and safeguarding user privacy and institutional interests within the digital environment.²

Cybersecurity is further defined as a coordinated set of legal and regulatory norms, operational procedures, and technical mechanisms, harmonized between the public and private sectors at both national and international levels, with the objective of protecting the digital environment. This field is grounded in ensuring the continuity of information systems, safeguarding digital privacy, preserving the confidentiality of data, and taking the necessary measures to protect individuals from various forms of cyber threats.³

Accordingly, cybersecurity can be understood as a suite of information systems designed to detect attacks or threats targeting the infiltration of information networks, with the purpose of safeguarding them and ensuring their integrity and operational continuity.

¹ - JOSHI Aditya, “*Study of Cybersecurity Laws and Regulation*”, Indian Journal of Law, Vol. 2 Issue 3, May - June 2024, p 07.

² - I.T.U.T (2008, April 18). X.1205: “Overview of cybersecurity”, available on website: www.itu.int

³ - MENAD Icherak, BELACEL Yasmine Bint Nabi, LAMRI Hakim, “*Legal Aspects of Cybersecurity*”, journal of legal and economic research, volume 7, number 2, 2024, p 946.

Second: the importance of cybersecurity

The importance of cybersecurity lies in its role as the first line of defense in protecting systems and information from digital attacks that may threaten the stability of individuals and institutions. It is not limited to securing personal data; rather, it ensures business continuity and maintains trust in the digital environment. Its significance can be summarized as follows:

- **Preserving institutional reputation:** It prevents breaches that could negatively affect the trust of clients and investors, thereby enhancing credibility in the market.
- **Ensuring the continuity of economic activity:** It mitigates the impact of cyber-attacks, such as ransom ware, which can paralyze systems and cause significant financial losses.
- **Maintaining operational continuity:** Cyber-attacks can disrupt a company's operational processes, leading to work stoppages and productivity losses. Therefore, having a robust cybersecurity strategy is essential for business continuity and reduces the likelihood of costly interruptions in commercial activities.⁴
- **Enabling secure remote work:** It allows employees to perform their tasks safely without exposing organizational data to risk.
- **Protecting sensitive information:** cybersecurity plays a central role in safeguarding sensitive data, including personal information, medical records, financial data, and intellectual property rights. In the absence of an effective cybersecurity system, institutions and individuals become vulnerable to breaches that may result in identity theft or financial fraud.⁵
- **Legal and regulatory compliance:** It helps institutions adhere to data protection laws, such as the General Data Protection Regulation (GDPR), and avoid penalties and fines.
- **Enhancing efficiency and productivity:** By reducing disruptions caused by cyber-attacks or malicious software, it ensures the smooth operation of processes.⁶

Second section: The Concept of Big Data

Big data is one of the most prominent concepts that has emerged with the rapid advancement of information and communication technologies, representing a

⁴ - NU Editorial Contributors. "What is cyber security and Its Importance to Business", National University, San Diego, USA, 2025, available at this website: <http://www.nu.edu/blog/what-is-cybersecurity>

⁵ - Sentinel One, "What Is Cyber Security? Types, Importance & Threats", 20 Aug. 2025. Available at: <http://www.sentinelone.com/blog/what-is-cyber-security-types-importance-threats>

⁶ - Ibid.

strategic resource in the era of digitalization. The expansion in the use of the internet and smart devices has generated enormous volumes of data that require new methods for storage, processing, and analysis. Accordingly, the concept of big data can be addressed by defining it **(first)**, outlining its distinctive characteristics **(second)** and highlighting its significance **(third)**.

First: Definition of Big Data

Big data refers to the enormous and complex volumes of information, both structured and unstructured, that flow continuously to institutions and are difficult to manage using traditional methods. Its true value lies in leveraging it through precise analysis to extract indicators and insights that support decision-making and enhance confidence in setting future strategies, thereby contributing to improved institutional performance and increased competitiveness.⁷ It represents an enormous volume of complex data whose size exceeds the capacity of traditional software and computational mechanisms to store, process, and distribute.

Second: characteristics of Big Data

Big data refers to information that is so large, fast, or complex that it is difficult or impossible to process using traditional methods. It is characterized by several features, which can be summarized as follows:

- **Volume:** Institutions collect data from diverse sources such as transactions, Internet of Things (IOT) devices, industrial equipment, visual and audio materials, social media platforms, and others. In the past, the cost of storing such data was prohibitively high; however, the emergence of data warehouses, Hadoop technology, and cloud computing has significantly alleviated this burden.
- **Velocity:** With the expansion of IOT technologies, data flows to institutions at high speed, requiring immediate processing. Radio-frequency identification (RFID) technologies, sensors, and smart meters have further increased the volume of data flow, necessitating near-instantaneous handling.⁸
- **Variety:** Data comes in multiple forms, ranging from structured digital data in traditional databases to unstructured text, emails, video clips, audio recordings, stock market indicators, and financial transactions.⁹

⁷ - SAS Institute Inc, “*Big Data: What It Is and Why It Matters*”, 2025. Available on website: www.sas.com

⁸ - SAS Institute Inc, op. cit.

⁹ - RUTUJA Ganesh More, SWAYAM Shashank Shah, PRASAD Thakordas Shaha, ALKA S Malewar, Artificial Intelligence and Big Data, PK Publications, India/ Brazil/ Kenya, 2025, p 21..

- **Variability:** Data flows are characterized by instability and may experience frequent and significant changes. This poses a challenge for institutions that need to monitor trending topics on social media and manage daily, seasonal, or event-driven data surges.¹⁰
- **Veracity:** This refers to the necessity of ensuring the quality, accuracy, and reliability of data, emphasizing the need for data cleaning, validation, and consistency checks, thereby guaranteeing that the resulting analyses achieve a high level of trustworthiness and dependability.¹¹

Third: The Importance of Big Data

The importance of big data is linked to how it is utilized rather than its sheer volume, as analyzing data from various sources can lead to a set of significant outcomes related to improving resource management and enhancing operational efficiency, in addition to identifying ways to develop products and support informed decision-making. When big data is integrated with high-performance analytics, it becomes possible to perform multiple tasks, including:

- Identifying the root causes of problems and malfunctions in a short time;
- Improving healthcare by rapidly converting medical imaging data into valuable indicators;
- Reassessing risks within a brief period;
- Increasing the accuracy of deep learning models in classification and their ability to adapt to changes;
- Predicting fraudulent behavior before it negatively affects the institution.¹²

Third section: The Concept of Artificial Intelligence

Artificial intelligence is among the most influential technologies in the global technological landscape, experiencing rapid expansion across various sectors due to its ability to enhance efficiency, improve service quality, and support decision-making in complex environments. Its widespread adoption has contributed to reshaping work and production methods in multiple fields, including healthcare, industry, education, cybersecurity, and financial services, making it a fundamental pillar in the digital transformation process. To provide a precise understanding of this concept, it is necessary to address its definition **(first)**, and significance **(second)**.

¹⁰ - SAS Institute Inc, op. cit.

¹¹ - RUTUJA Ganesh More, SWAYAM Shashank Shah, PRASAD Thakordas Shaha, ALKA S Malewar, p 22.

¹² - SAS Institute Inc, op. cit.

First: Definition of Artificial Intelligence

Artificial intelligence is defined as the science concerned with building systems capable of performing actions that would be considered intelligent if carried out by humans. It is described as systems capable of perceiving their environment and making decisions that maximize their chances of achieving their objectives. This definition is based on the principle of rational behavior rather than the simulation of human consciousness, positioning artificial intelligence as a field aimed at designing mechanisms capable of thinking and making decisions logically and effectively based on available information.¹³

Second: The Importance of Artificial Intelligence

The importance of artificial intelligence is evident across numerous fields due to its effective role in automating tasks;¹⁴ it also enhances data analysis capabilities to support decision-making, enables personalization, and drives innovation in areas such as healthcare, environmental protection, and information engineering. The significance of artificial intelligence can be detailed as follows:

- **Enhancing automation and efficiency:** Artificial intelligence contributes to automating repetitive tasks, increasing productivity, and allowing employees to focus on strategic activities;
- **Advanced data analysis:** Artificial intelligence possesses exceptional ability to process big data and extract patterns and accurate insights, thereby strengthening data-driven decision-making;
- **Enabling personalization:** It allows companies to provide services and experiences tailored to user behavior and preferences.
- **Innovation and solving complex problems:** It plays a pivotal role in addressing global challenges in fields such as advanced medicine, diagnostics, and smart agriculture.¹⁵
- **Information engineering:** By improving the user experience through facilitating access to information and executing tasks efficiently, making content accessible to a broader range of users.

Second requirement: The Dual Impact of Artificial Intelligence on the cybersecurity System

Artificial intelligence plays a pivotal role in contemporary digital systems due to its capacity to process vast volumes of data and identify patterns that remain

¹³ - STUART Russell Stuart, NORVIG Peter, Artificial Intelligence: A Modern Approach. Third ed., Pearson, 2010, p 2.

¹⁴ - Automation refers to the use of systems and artificial intelligence technologies to perform tasks and processes without direct human intervention.

¹⁵ - BERNARD Marr, "what Is the importance of artificial intelligence (AI)", available on website: <https://bernardmarr.com>

undetectable by conventional methods. This technological advancement has empowered cybersecurity authorities to develop more precise and efficient mechanisms for monitoring and mitigating attacks, thereby strengthening protection across diverse sectors. Nonetheless, cybercriminals have rapidly identified the potential of artificial intelligence and have employed it to conduct increasingly sophisticated and innovative attacks, often imperceptible through traditional detection methods. Consequently, artificial intelligence functions as a double-edged sword: it is utilized by malicious actors to facilitate cyber-attacks, while simultaneously serving as a tool to enhance the cybersecurity of big data systems.

This section addresses the dual impact of artificial intelligence on cybersecurity by examining AI facilitated cyber-attacks **(first section)** and highlighting AI's role in augmenting the effectiveness of big data cybersecurity **(second section)**.

First section: AI-Supported Cyber-Attacks on Cybersecurity

Contemporary digital environments are experiencing a marked increase in the deployment of artificial intelligence, resulting in a profound transformation in the landscape of cybercrime. Advanced AI algorithms are leveraged to design offensive strategies exhibiting heightened adaptability and stealth within information systems. Such attacks systematically analyze the digital environment, pinpoint specific vulnerabilities, and exploit them with efficiency, while simulating human behavior to obfuscate monitoring systems and diminish the likelihood of detection.

These attacks continuously adapt their strategies in response to security system countermeasures, leading to advanced forms of cyber-attacks on big data cybersecurity, including smart phishing attacks **(first)**, adaptive malware **(second)**, automated vulnerability detection **(third)**, and deepfake technologies **(fourth)**.

First: Smart Phishing Attacks

Smart phishing attacks refer to AI-driven techniques that create highly convincing fraudulent messages based on the analysis of user behavior. Artificial intelligence enables attackers to produce targeted phishing messages with a high level of personalization, making them more persuasive and increasing their likelihood of success. By analyzing individuals' online behavior and communication patterns, algorithms can generate content that closely resembles legitimate messages, making it difficult for users and sometimes even security systems to distinguish between automatically generated fraudulent messages and genuine correspondence.¹⁶

¹⁶ - Steve Wilson, "Cybersecurity and Artificial Intelligence: Threats and Opportunities", Contrast Security, available at: www.contrastsecurity.com

Second: Adaptive Malware

Adaptive malware refers to a type of malicious software that relies on machine learning and artificial intelligence techniques to adjust its behavior according to the environment of the system it infiltrates. This malware is characterized by its ability to monitor the protection mechanisms within the system and continuously modify its mode of operation to ensure its activity persists without being detected.

As a result of this continuous adaptation, such malware becomes more difficult to detect and neutralize compared to traditional malware that relies on static, unchanging code. It is capable of altering its structure and operational mechanisms in response to the security measures it encounters, and it benefits from interacting with its digital environment to change execution methods and attack paths in real time, enabling it to evade signature-based detection systems and conventional security solutions.¹⁷

Third: Automated Vulnerability Detection

Automated vulnerability detection is carried out by performing precise and rapid scans of systems and applications using artificial intelligence techniques to identify security vulnerabilities and potential weaknesses before they are exploited. The danger of these tools lies in the fact that cybercriminals can also use them to analyze the operational and technical structure of institutions and then pinpoint areas with weak protection. This enables the launch of more accurate and effective attacks, based on a deep understanding of security flaws that traditional methods may not detect with the same speed.¹⁸

Fourth: Deep Fake Technologies

Deep fake technologies, which rely on artificial intelligence, allow the production of highly realistic images, videos, and audio recordings that are entirely fabricated. Criminals may exploit this content to impersonate real individuals or to spread misleading information, which undermines public trust and causes extensive reputational damage at both the individual and institutional levels, in addition to harming information security.¹⁹

¹⁷ - Digital XRAID, “*Adaptive Malware: The Next Evolution of Cyber Threats & How to Defend against It*”, available at: www.digitalxraid.com

¹⁸ - Steve Wilson, op. cit, p 27.

¹⁹ - Ibid.

Second section: The Role of Artificial Intelligence in Enhancing Big Data cybersecurity

Artificial intelligence plays a significant role in strengthening the cybersecurity of big data through its various techniques related to machine learning and data analysis, which are fundamental in countering emerging cyber threats. AI enables security systems to process vast amounts of data in real time, detect unusual patterns or behaviors, and take automated and rapid actions upon identifying any potential risk.

Some key AI techniques that contribute to enhancing cybersecurity include predicting cyber threats before they occur (**first**), automated response to cyber threats (**second**), and combating toxic and malicious data (**third**).

First: Predicting Cyber Threats Before They Occur

Machine learning based on artificial intelligence is one of the most prominent intelligent tools capable of supporting security systems in predicting cyber threats before they materialize. These algorithms analyze vast amounts of historical data related to past attacks, extracting recurring patterns, behaviors, and relationships that precede threats. Through continuous analysis, machine-learning systems can detect unusual changes in network behavior or in how users interact with systems, which may indicate hostile activity in its early stages.

Furthermore, AI can predict potential attack scenarios based on knowledge learned from previous incidents, enabling institutions to implement proactive defensive measures. As a result, cybersecurity shifts from a reactive model, responding after a threat occurs, to a proactive model based on anticipation and prevention, thereby enhancing protection effectiveness and reducing the likelihood of successful attacks.²⁰

Second: Automated Response to Cyber Threats

Automated response to cyber threats is a pivotal step in the development of digital protection systems, aiming to shift from traditional methods that rely on human intervention to mechanisms that operate fully autonomously. This shift is necessitated by the accelerating and complex nature of modern attacks, where the time available for threat analysis and decision-making no longer supports manual responses.

²⁰ - SHAHROUZ Mehdi, NAZARI Ali, and MORADI Sara, “*AI-Driven Cybersecurity: Legal and Ethical Considerations in Autonomous Systems Protecting Digital Networks*,” *Legal Studies in Digital Age*, Volume 2, Issue 1, 2023, p 3.

Within this framework, artificial intelligence enables security systems to take immediate action upon detecting any suspicious activity without waiting for human evaluation or guidance. Systems can isolate infected devices or servers to prevent the spread of damage, halt unauthorized communications, and activate additional defenses as needed. The key advantage of this approach is the reduction of the time between threat detection and response, which is critical in environments where attacks can escalate within seconds. Automated response also ensures higher accuracy and consistency, as it minimizes the likelihood of human error and provides a coordinated and effective reaction every time.²¹

Third: Combating Toxic and Adversarial Data

Toxic and adversarial data refer to ordinary data that are exploited or manipulated in ways that lead to incorrect decisions or misleading classifications, posing a genuine threat to the integrity of systems that rely on them. The danger of such attacks is particularly evident in so-called hostile environments, where attackers introduce subtle, imperceptible changes to the data during either the training or testing phases.

In the case of toxic attacks, the attacker corrupts a portion of the training data, causing the model to learn biased or misleading information that later results in improper behavior. Adversarial attacks, on the other hand, focus on deceiving the model during actual operation by injecting carefully modified samples capable of fooling networks into incorrect classification, even though the alterations may be imperceptible to the naked eye. To counter these risks, a variety of defensive strategies are developed, including improving training data quality, modifying the internal architecture of models, and adding protective layers that activate upon detecting suspicious data, thereby enabling the detection and prevention of toxic data.²²

²¹ - Ibid.

²² - - SHAHROUZ Mehdi, NAZARI Ali, and MORADI Sara, op. cit, p 3.

THE SECOND TOPIC:

THE LEGAL FRAMEWORK OF CYBERSECURITY IN LIGHT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND BIG DATA

The technological evolution driven by artificial intelligence and big data is reshaping work environments, economies, and public services, while simultaneously generating new forms of risks both in terms of the increasing complexity of cyber-attacks and the smart tools provided by AI that enable system breaches and data exploitation in various ways.

In light of these transformations, the adoption of national and international cybersecurity laws has become an imperative, driven by rapid technological changes that have redefined the nature of digital threats and risks. The continuous advancement of AI technologies, the widespread use of big data, and the digital transition of various sectors have created a complex cyberspace that transcends national boundaries and amplifies the likelihood of sophisticated attacks that cannot be addressed through technical measures alone.

With the rise in cyber intrusions, the growing professionalism of cybercriminals, and the increasing international interconnectedness of networks, it has become essential to establish comprehensive legal frameworks that define responsibilities, set security standards, regulate the use of digital tools, and strengthen cross-border cooperation. Accordingly, this chapter examines national cybersecurity laws in the context of AI development (**first requirement**) and then highlights the various international conventions governing the field (**second requirement**).

First requirement: National Laws Regulating cybersecurity in Light of the Development of Artificial Intelligence and Big Data

Algeria has experienced a gradual evolution in its legal framework for cybersecurity and data protection, starting with Law number 09-04, which criminalized attacks on automated data processing systems (**first section**), and followed by Law number 18-07 on the prevention of crimes related to information and communication technologies (**second section**). This development culminated in Law number 25-11 regulating the protection of personal data and the authorities responsible for securing information systems (**third section**), alongside the relevant provisions of the Penal Code in this area (**fourth section**).

First section: Law number 09-04 on the Special Rules for the Prevention and Combat of Crimes Related to Information and Communication Technologies

Law number 09-04 on the special rules for the prevention and combat of crimes related to information and communication technologies²³ is considered the first Algerian legislative law that comprehensively and securely regulates the prevention and prosecution of system breaches and criminal exploitation of technology. This law contains a set of provisions aimed at protecting the state and citizens from cyber threats and its main contents can be summarized as follows:

- Providing precise definitions for concepts related to information and communication technology (such as information systems, electronic data, and communication data) to determine the scope of the law;
- Regulating the legal monitoring of electronic communications, allowing authorities to supervise messages or communications under specific conditions in a legally guaranteed manner;
- Permitting the inspection of information systems to obtain digital data and make copies of content while ensuring the integrity of the original data;
- Establishing technical mechanisms to block or prevent access to certain data if its content is suspected of constituting a crime;
- Restricting the use of data collected through monitoring so that it is limited to investigations and judicial procedures, preventing its use for unauthorized purposes;
- Imposing obligations on communication and technology service providers to support judicial investigations by cooperating in the collection or recording of data while respecting confidentiality and privacy protection;
- Requiring service providers to retain traffic data (such as sender identity, connection time, sender and recipient, type of service, etc.) for a specified period to ensure the verification of operations and criminal enforcement;
- Establishing a specialized national authority called the National Authority for the Prevention of Crimes Related to Information and Communication Technology, tasked with coordinating between judicial and security entities, preventing cybercrime, and providing technical advice in the field of digital technology.²⁴

²³ - Law no. 09-04 of 14 sha'ban 1430 corresponding to august 5, 2009, on Specific Rules on the Prevention and Fight against information technologies and communication's crimes, published in official gazette of the people's democratic republic of Algeria, no. 47, 16 august 2009.

²⁴ - See articles 14 and 15 of the same reference.

- Organizing international judicial cooperation in combating cybercrime, enabling the exchange of digital evidence and the provision of mutual legal assistance between states;
- Defining the jurisdiction of the Algerian judiciary over cybercrimes even if committed outside Algerian territory, provided they affect the interests of the state or its cybersecurity.²⁵

Second section: Law Number 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Law number 18-07 constitutes the Algerian legislative framework dedicated to regulating the protection of natural persons in the processing of personal data. It was enacted to establish clear rules ensuring respect for privacy in light of the widespread digital processing of data, defining principles for the use of personal information, mechanisms for its supervision, and guarantees for individuals against public and private entities that collect, store, or exploit data. The main contents of this law include:

- Providing precise definitions for personal data, processing, data controllers, and data processors;
- Establishing fundamental principles for data processing, including transparency, proportionality, legality, and specific purpose;
- Determining the circumstances under which data collection and processing are permitted, with clear requirements for the explicit and unambiguous consent of the data subject;²⁶
- Imposing obligations on entities that process data, such as securing the data, ensuring its confidentiality, and preventing its use for unauthorized purposes;
- Granting individuals fundamental rights, including the right of access, correction, objection, and erasure of data when the reasons for its retention no longer exist;
- Regulating the transfer of personal data abroad, linking it to legal guarantees that ensure protection equivalent to that provided nationally;
- Establishing an independent national authority responsible for oversight, ensuring compliance with the law, authorizing sensitive processing activities, and adjudicating complaints²⁷;
- Establishing a system of administrative and criminal penalties to ensure deterrence in case of violations of data protection rules.²⁸

²⁵ - See articles 15,16 and 18 of the law number 09-04, op.cit.

²⁶ - See article 7 of the law no 18-07 of 25 Ramadan 1439, corresponding to 10 June 2018, relating to the protection of natural persons in the processing of personal data, published in the official gazette of the people's democratic republic of Algeria, no 34 of 2018.

²⁷ - See articles 25 of the same reference.

Third section: Law number 25-11 Amending and Supplementing Law no 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Law number 25-11 was enacted to amend and supplement the provisions of Law number 18-07 concerning the protection of natural persons in the processing of personal data, with the aim of strengthening the national legal framework and ensuring its alignment with technological developments and privacy protection requirements. This law introduced a set of substantive amendments that enhance the guarantees provided to individuals and clarify the responsibilities of data-processing entities, including:

- Strengthening the definitions of certain processing-related concepts to clarify the scope of the law and refine technical and legal terminology;²⁹
- Obligation to appoint a Data Protection Officer;³⁰
- Establishing stricter conditions for data collection by emphasizing the necessity of free and explicit consent, and expanding cases in which the data processor must provide accurate information to the data subject prior to any processing;
- Strengthening the framework for sensitive data by introducing additional controls for its processing, ensuring greater protection for special categories of data;
- Enhancing the rights of data subjects by simplifying procedures for exercising access, correction, objection, and erasure, and obliging the processor to respond within shorter and clearer timeframes;
- Expanding the powers of the national authority by adding new responsibilities related to oversight, issuing authorizations, handling complaints, and imposing penalties;
- Tightening the penalty system by increasing fines and broadening the scope of criminalized acts, particularly regarding unauthorized processing or illegal transfer of data abroad;
- Clarifying the rules for data transfer outside Algeria by incorporating additional conditions regarding the adequacy of protection levels in recipient countries.³¹

²⁸ - See articles 65 of the same reference.

²⁹ - See article 3 of law no 25-11 of 28 Moharram 1447 corresponding to 24 July 2025 amending and supplementing law no 18-07 of 25 Ramadan 1439 corresponding to 10 June 2018 relating to the protection of natural persons in the processing of personal data, published in the official gazette no 48 of 24 July 2025.

³⁰ - See article 41 bis of the same reference.

³¹ - See article 45 bis 13 and article 45 bis 14 of the same reference.

Fourth Section: Provisions related to Cybersecurity in the Algerian Penal Code

The Algerian Penal Code demonstrates a clear legislative trend toward strengthening the deterrent framework for cybersecurity, by addressing a range of issues related to the protection of information systems, digital data, and individuals' privacy through digital means. These provisions reflect the legislator's awareness of emerging threats and provide a legal basis for addressing acts targeting information systems or exploiting the cyberspace. The main aspects can be summarized as follows:

- 1- Protection of the integrity of information systems:** by criminalizing all acts aimed at compromising the functions of digital systems or disrupting their operation, including:
 - Unauthorized access to or presence within automated data processing systems;
 - Disruption or partial or total sabotage of system operations;
 - Deletion or alteration of data stored or transmitted through electronic media.
- 2- Combating offenses against digital data:** by deterring any conduct aimed at compromising automated data processing systems, manipulating, or misappropriating data through fraudulent means, including:
 - Fraudulent input of data into information systems;
 - Unauthorized modification or deletion of digital data;
 - Illegal use or trafficking of data.³²
- 3- Criminalization of offenses against privacy via electronic means:** by protecting digital privacy as an extension of personal sanctity, including:
 - Criminalizing the capture, recording, transmission, or publication of personal information or images without the owner's consent;
 - Protecting personal data from any use that violates the confidentiality or privacy of its owners.³³
- 4- Addressing certain forms of cybercrime of a fraudulent nature:** by criminalizing common behaviors in the digital environment, including:
 - Criminalizing certain forms of information fraud;
 - Criminalizing acts related to harvesting, providing, or publishing data for unlawful purposes.³⁴

It can be concluded from the study that the Algerian legislator has organized aspects related to cyber security within the framework of specific and general laws;

³²- See articles 394 bis to 394 bis 7 of the law no 66-156 dated 8 June 1966 relating to the Penal Code, official gazette no 49 issued on 8 June 1966, amended and supplemented.

³³ - See articles 303 bis to 303 bis 3 of the same reference.

³⁴ - See articles 379 bis to 379 bis 1 of the same reference.

however, the issue of artificial intelligence has not yet been addressed despite its rapid development and widespread use in various fields, which constitutes a legal gap that must be considered. Given the urgent need to regulate the diverse uses of AI technologies in Algeria, the "National Scientific Council for Artificial Intelligence" was established based on a joint ministerial proposal between the Ministry of Higher Education and Scientific Research on one hand, and the Ministry of Knowledge Economy and Startups on the other. The council is described as an advisory body tasked with proposing public policies and providing strategic insights. It plays a pivotal role by assessing the national AI environment, studying potential risks, proposing standards to ensure safe and responsible utilization, contributing to enhanced coordination between government entities, the academic sector, and the economic sector, and paving the way for the preparation of more comprehensive future legislation addressing governance, responsibility, and rights protection in the field of artificial intelligence.³⁵

On the other hand, the study indicated that Algeria has relied on a deterrence-based approach by combating cybercrime; however, this is not sufficient. The country needs to move from the stage of deterrence and punishment to a stage of smart data governance, meaning the establishment of legislation that regulates the legitimate use of artificial intelligence in a way that ensures cybersecurity in the context of reliance on big data.

It is worth noting that, in light of the rapid evolution of artificial intelligence and big data technologies, a fundamental challenge emerges in the temporal gap between the dynamism of technological innovation and the slowness of the traditional legislative process. By virtue of its procedural nature and the complexity inherent in the stages of enacting and amending laws, the legislative system often moves at a pace far slower than that of technological transformations, thereby resulting in regulatory gaps or in the continued application of provisions that no longer reflect the actual technological reality.

Moreover, legal texts of a detailed nature, drafted in response to a specific technology or particular technical context, are liable to become rapidly obsolete once new applications or more advanced models emerge, which limits their effectiveness in addressing constantly evolving and emerging cyber risks. Accordingly, the effectiveness of national legislation is no longer solely dependent on increasing the number of statutory provisions or intensifying penalties, but rather on adopting a set of legislative adaptation mechanisms for cybersecurity in response to the accelerated development of artificial intelligence and big data, as follows:

³⁵ - AI Council, "Driving Innovation in AI for a Smarter Algeria", available on the website: www.aicouncil.dz

- **Ensuring the flexibility and adaptability of national laws:** The flexibility and adaptability of national legislation constitute a fundamental key to ensuring that legal frameworks keep pace with the rapid developments in the field of artificial intelligence and big data. This mechanism requires a shift from “rigid regulation” to regulation grounded in general principles that can be readily applied despite the diversity of technical models and future scenarios. This approach, referred to as adaptive regulation, enables laws to adjust to technological developments without undermining the core guarantees for the protection of rights and public interests. It emphasizes the capacity of the legal framework to be revised in accordance with periodic risk assessments and the level of technological advancement, thereby contributing to bridging the gap between the speed of innovation and the slowness of the traditional legislative process.³⁶
- **Adopting a risk-based regulatory approach:** This approach is founded on classifying artificial intelligence systems according to levels of risk and imposing obligations proportionate to each level, ranging from the complete prohibition of unacceptable systems to lighter compliance requirements for low-risk systems, while subjecting high-risk systems to strict oversight. It further entails the gradual implementation of reform in a manner that balances protection with the promotion of innovation.³⁷
- **Empowering the competent regulatory authorities to update implementing regulations in a periodic and expeditious manner:** This requires granting the relevant bodies the authority to issue adaptive implementing regulations grounded in up-to-date data concerning emerging technologies, while incorporating structured mechanisms for periodic review and organized feedback. It also entails making use of advanced analytical tools to support decision-makers, thereby ensuring a prompt response to emerging risks without undermining the legitimacy of the legal framework.³⁸

³⁶ - Anka Reuel, Trond Arne Undheim, “Generative AI Needs Adaptive Governance”, arXiv (preprint), June 6, 2024, available at the website : <https://doi.org/10.48550/arXiv.2406.04554>

³⁷ - Abhishek Singh, *Adaptive Legal Frameworks for AI Governance: Bridging Innovation and Security in Emerging Economies*, African journal of biomedical research, Vol. 27, December 2024, p 1286.

³⁸ - Ibid. p1289.

Second requirement: International Instruments Regulating Cybersecurity in Light of the Development of Artificial Intelligence and Big Data

The cyberspace, characterized by its cross-border nature, the interconnection of actors, and the difficulty of containing threats within a single sovereign domain, has created an urgent need for international cooperation to ensure the stability of digital transactions, coordinate efforts in combating cybercrime, and unify fundamental principles for protecting information infrastructures, thereby enhancing trust and security in the global digital environment. In this section, we will address the international legal framework governing cyber security in light of the development of artificial intelligence and big data by examining binding agreements in the field, notably the Budapest Convention **(first section)** and the United Nations Convention on Cybercrime of 2024 **(second section)**. We also consider non-binding reference instruments, including the European General Data Protection Regulation (GDPR) **(third section)** and UNESCO's recommendations on the ethics of artificial intelligence **(four section)**.

First section: Budapest Convention

The Budapest Convention on Cybercrime constitutes the most comprehensive international framework for regulating cybersecurity, as it established unified rules for criminalizing acts that compromise the integrity of systems and data. It also set procedural mechanisms for investigation and the collection of digital evidence, in addition to creating an advanced system for international cooperation to address cross-border threats. Its significance lies in being the first binding international instrument that addresses cybercrime comprehensively, making it a fundamental reference for countries in developing their national legislation and enhancing their capabilities to protect the digital space. Its main substantive provisions can be summarized as follows:

- Criminalizing unauthorized access to information systems;
- Criminalizing the illegal interception of digital communications;
- Protecting data integrity by criminalizing intentional destruction, alteration, deletion, or damage;
- Safeguarding the integrity of information systems by criminalizing acts that disrupt services or harm digital infrastructures;
- Criminalizing the misuse of tools and software designed to commit cybercrimes;
- Criminalizing information forgery related to creating false data or altering correct data;

- Criminalizing information fraud aimed at obtaining unlawful benefits through digital systems;³⁹
- Establishing specific procedural rules for digital evidence, including the urgent preservation of data, its disclosure, and the cross-border execution of digital procedures;
- Regulating the criminal use of modern technologies, including artificial intelligence, through provisions on prevention, monitoring automated systems, and combating the generation of fraudulent or misleading content;
- Strengthening international cooperation in cross-border investigations through the exchange of digital data, mutual legal assistance, and activating specialized technical communication channels.⁴⁰

It is evident from analyzing the content of the Budapest Convention on Cybersecurity that it represents a prominent legal framework aiming to ensure the security of cyberspace and to unify the fundamental principles for combating cybercrimes in a rapidly evolving digital environment.

Second section : United Nations Convention on Cybercrime, 2024

The United Nations Convention on Cybercrime represents a modern international framework that addresses the nature of contemporary digital transformations. It aims to protect cybersecurity, ensure data integrity, and regulate the risks associated with advanced technologies such as artificial intelligence. Its provisions enhance states' capabilities to confront cybercrime by establishing substantive and procedural rules that safeguard information infrastructures, secure the flows of big data, and counter the criminal use of intelligent systems. The key provisions of the convention related to these aspects include:

- Criminalizing unauthorized access to information systems;
- Criminalizing unlawful interference with data, including destruction, alteration, or disruption;
- Criminalizing interference with information systems that leads to their disruption or shutdown;
- Criminalizing the misuse of digital tools and software designed to commit illegal cyber acts;
- Criminalizing information forgery involving the creation of fake data or manipulation of authentic data;
- Criminalizing cyber fraud that exploits digital data processing to gain unlawful benefits;

³⁹ - See articles 2 to 8 of the convention on cybercrime (Budapest convention), council of Europe, 23 Nov 2001, available on the website: www.coe.int

⁴⁰ - See articles 23, 25 and 35 of the same reference.

- Regulating the protection of personal data and big data through provisions related to information confidentiality, storage, and lawful use;⁴¹
- Establishing procedural rules for digital evidence, including the urgent preservation of data, its disclosure, and the cross-border execution of digital procedures;
- Regulating the criminal use of modern technologies, including artificial intelligence, through specific provisions on prevention, monitoring automated systems, and combating the generation of fraudulent or misleading content;
- Enhancing international cooperation in cross-border investigations through the exchange of digital data, mutual legal assistance, and the activation of specialized technical communication channels.

Therefore, we can say that the United Nations Convention on Cybercrime provides a comprehensive legal framework linking cybersecurity with the protection of big data and mitigating risks arising from artificial intelligence. This makes it a global reference for countries to adopt an effective legal framework aimed at safeguarding cyberspace from related threats and crimes, especially in light of the rapid development of AI technologies and the growing volume of big data. Algeria signed this convention on October 25, 2025, establishing a cooperative framework that strengthens the country's capacity to confront cross-border threats, although the international legal ratification process is still subject to its own procedures.

Third section: The European General Data Protection Regulation (GDPR)

The European General Data Protection Regulation (GDPR) constitutes an advanced legal framework for regulating digital data processing amid increasing cybersecurity risks, the expansion of big data flows, and growing reliance on artificial intelligence technologies. The regulation establishes precise rules to ensure compliance with the principles of lawfulness, transparency, and accountability in all processing activities. It imposes a set of obligations that contribute to enhancing cybersecurity and protecting systems dependent on data, through strict security requirements, mandatory risk assessments, and safeguards for the protection of individuals' digital rights. The GDPR addresses, among other aspects:

- Data protection principles and conditions for lawful processing;⁴²

⁴¹ - See articles 6 to 14 of the United Nations convention against cybercrime: strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, United Nations, 2024, available on website: www.unodc.org

⁴² - See articles 5 and 6 of the General Data Protection Regulation (GDPR), regulation number 2016/679 of the European Parliament and of the Council of 27 April 2016, official journal of the European Union, 4 May 2016.

- Cybersecurity measures required for controllers and processors;
- Notification in the event of a data breach;⁴³
- Data protection by design and by default;
- Data protection impact assessment for high-risk systems, including AI applications;
- Regulation of decisions based on automated processing, including AI systems.⁴⁴

Accordingly, we can say that the European General Data Protection Regulation (GDPR) represents a comprehensive legal framework that focuses on data protection, enhancing digital security, and regulating the use of smart technologies within a legal environment that safeguards individuals and fosters trust in the European digital space. Although it is not binding for countries outside Europe, it serves as an excellent reference in the field.

Fourth Section: UNESCO'S Recommendations on the Ethics of Artificial Intelligence

UNESCO's Recommendations on the Ethics of Artificial Intelligence aim to regulate the responsible use of intelligent technologies within a digital environment characterized by the extensive application of automated processing and the increasing challenges of safeguarding human values. They also seek to balance innovation with protection, ensuring that intelligent systems do not become tools that threaten dignity, justice, or security. The content of these recommendations, which govern the relationship between artificial intelligence and human societies, includes:

- Respect for human rights and human dignity;
- Equality and non-discrimination in the design and use of intelligent systems;
- Promoting social justice and ensuring access to technology for all;
- Ensuring transparency and interpretability in algorithms;
- Ensuring cybersecurity and data protection in AI-based systems;
- Accountability for damages resulting from the use of intelligent systems;
- Human oversight over automated decision-making processes;
- Promoting environmental sustainability throughout the lifecycle of artificial intelligence.⁴⁵

⁴³ - See articles 32, 33, and 34 of the General Data Protection Regulation (GDPR), op. cit.

⁴⁴ - See article 22 of the same reference.

⁴⁵ - UNESCO, "*recommendation on the ethics of artificial intelligence*", 2021, available on the website: www.unesdoc.unesco.org

It can be concluded that these recommendations seek to balance technological development with the protection of the digital environment, thereby promoting ethical values and safeguarding humans from the threats posed by increasingly sophisticated technological tools. They call for ensuring cyber security in AI-based systems and emphasize the necessity of human oversight over automated decisions due to their potential impact on individuals and societies.

It is worth noting that, despite the growing importance of international instruments in regulating the digital sphere, their adequacy in addressing cybersecurity risks associated with artificial intelligence remains relative and limited. Existing conventions, such as the Budapest Convention on Cybercrime, primarily focus on the criminalization of traditional criminal acts within the digital environment, without directly addressing the specific challenges posed by artificial intelligence systems, such as liability for automated decisions or the risks arising from self-learning generative systems.

More recent instruments, such as the United Nations Convention against Cybercrime, seek to broaden the scope of international cooperation; however, they remain largely anchored in a crime-control logic rather than in regulating the life cycle of artificial intelligence systems as such. Similarly, both the General Data Protection Regulation and the UNESCO Recommendation on the Ethics of Artificial Intelligence provide an important normative framework grounded in the protection of fundamental rights and ethical principles. Nevertheless, their general or advisory nature limits their capacity to comprehensively govern all emerging technical risks. Accordingly, while these instruments lay an important international normative foundation, they do not constitute a comprehensive and integrated framework for regulating the intersection between artificial intelligence and cybersecurity, thereby highlighting the need for more specialized rules and deeper international coordination consistent with the cross-border nature of these technologies.

In light of the shortcomings revealed by the current international framework, it becomes necessary to move beyond critical assessment toward the formulation of structural reforms more consistent with the complex and evolving nature of artificial intelligence. This may be achieved through the development of a complementary and specialized international instrument addressing the intersection of artificial intelligence and cybersecurity through a comprehensive approach covering the entire life cycle of systems from design and training to deployment and subsequent monitoring while incorporating minimum technical standards for risk management, clear transparency requirements, and mechanisms for determining liability. It is also necessary to move beyond the traditional criminal-law paradigm toward a preventive and anticipatory approach based on mandatory risk impact assessments, the integration of cybersecurity requirements by design, and the adoption of international accreditation or certification schemes for high-risk systems.

Such reform further requires strengthening the binding character of international instruments through periodic monitoring mechanisms and specialized coordinating bodies to ensure consistency between legal standards and technical specifications. Moreover, due consideration must be given to the digital divide among States by incorporating mechanisms for capacity-building and technology transfer, so that international standards do not become an obstacle to emerging economies. In this way, it becomes possible to move from a fragmented and weakly enforced international framework toward a more integrated and effective system for managing cybersecurity risks associated with artificial intelligence at the transnational level.

Conclusion:

This study highlights that structuring cybersecurity within the framework of artificial intelligence and big data has become an imperative to restore legal equilibrium in the governance of the digital environment. The increasing reliance on intelligent systems and large-scale data flows compels national and international legislators to develop new approaches that address emerging risks and safeguard individuals' fundamental rights. Despite numerous legislative initiatives aimed at enhancing protection in cyberspace, the core challenge remains how to establish rules capable of keeping pace with technological developments while balancing innovation with the protection of public and individual interests. The primary requirement today is to formulate a balanced and comprehensive legal framework that reinforces digital trust, secures cyberspace, and simultaneously preserves human dignity in a world governed by algorithms and driven by data. Based on the analysis of national and international legal systems in this field, the following recommendations are proposed:

- Strengthen the national legislative framework by enacting specific laws related to artificial intelligence and cybersecurity that account for the evolution of cybercrime and AI-related challenges, while ensuring alignment with contemporary international standards;
- Include in this legislation the establishment of an independent national authority specialized in artificial intelligence, tasked with monitoring ethical usage, supervising high-risk applications, and issuing technical and legal guidelines to ensure compliance;
- Develop a comprehensive national cybersecurity strategy that incorporates mechanisms for coordination between government agencies and the private sector, clearly defining roles and responsibilities in protecting digital infrastructures and critical data;
- Enhance the protection of personal data by updating national mechanisms for processing, retention, and transfer in accordance with leading international standards, particularly concerning big data safeguards;
- Develop technical and human capacities through specialized training programs in cybersecurity and artificial intelligence;

- Engage in international agreements on combating cybercrime, exchanging digital evidence, and safeguarding the digital space, thereby promoting cross-border cooperation and reducing impunity ;
- Establishing an adaptive national legislative model grounded in risk management, enabling the flexible updating of legal rules in line with the evolution of artificial intelligence and big data technologies, thereby ensuring the reduction of the gap between the speed of innovation and the slowness of the legislative process while preserving the protection of rights and cybersecurity;
- Working toward the development of a complementary and specialized international instrument that moves beyond the traditional criminal-law approach established by the aforementioned international conventions, by creating a comprehensive framework regulating the life cycle of artificial intelligence systems and strengthening international coordination in the management of cybersecurity risks.

Bibliography List:

1. Books

- RUTUJA Ganesh More, SWAYAM Shashank Shah, PRASAD Thakordas Shaha, ALKA S Malewar, Artificial Intelligence and Big Data, PK Publications, India/ Brazil/ Kenya, 2025.
- STUART Russell Stuart, NORVIG Peter, Artificial Intelligence: A Modern Approach. Third edition, Pearson, 2010.

2. Journal article :

- Abhishek Singh, “*Adaptive Legal Frameworks for AI Governance: Bridging Innovation and Security in Emerging Economies*”, African journal of biomedical research, Vol. 27, December 2024, p 1286. pp 1282-1295
- JOSHI Aditya, “*Study of cyber security Laws and Regulation*”, Indian Journal of Law, Vol. 2 Issue 3, May - June 2024, (p p 7-14).
- MENAD Icherak, BELACEL Yasmine Bint Nabi, LAMRI Hakim, “*Legal Aspects of cyber security*”, journal of legal and economic research, volume 7, number 2, 2024, p945 -963.
- SHAHROUZ Mehdi, NAZARI Ali, and MORADI Sara, “*AI-Driven Cybersecurity: Legal and Ethical Considerations in Autonomous Systems Protecting Digital Networks*, Legal Studies in Digital Age, Volume 2, Issue 1, 2023.
- Steve Wilson, “*cyber security and Artificial Intelligence: Threats and Opportunities*”, Contrast Security, n.d., available at: contrastsecurity.com.

3. Internet websites:

- Anka Reuel, Trond Arne Undheim, “*Generative AI Needs Adaptive Governance*”, arXiv (preprint), June 6, 2024, available at the website : <https://doi.org/10.48550/arXiv.2406.04554>.
- BERNARD Marr, “*what Is the importance of artificial intelligence (AI)*”, available on website: <https://bernardmarr.com>
- Digital XRAID, “*Adaptive Malware: The Next Evolution of Cyber Threats & How to Defend against It*”, available at: www.digitalxraid.com
- I.T.U.T (2008, April 18). X.1205: “Overview of cyber security”, available on website: www.itu.int
- NU Editorial Contributors. “*What is cyber security and Its Importance to Business*”, National University, San Diego, USA, 2025, available at this website: www.nu.edu
- SAS Institute Inc, “*Big Data: What It Is and Why It Matters*”, 2025. Available on website: www.sas.com
- Sentinel One, “*What Is Cyber Security? Types, Importance & Threats*”, 20 Aug. 2025. Available at: www.sentinelone.com

4. Legal texts:

International Conventions and Agreements Ratified by Algeria

- Convention on cybercrime (Budapest convention), council of Europe, 23 Nov 2001, available on the website: www.coe.int
- United Nations convention against cybercrime: strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, United Nations, 2024, available on website: www.unodc.org

Algerian laws and regulations

- Law no 66-156 dated 8 June 1966 relating to the Penal Code, JORA n ° 49 issued on 8 June 1966, amended and supplemented.
- Law no. 09-04 of 14 sha’ban 1430 corresponding to august 5, 2009, on Specific Rules on the Prevention and Fight against information technologies and communication’s crimes, published in JORA n ° 47, 16 august 2009.
- Law no 18-07 of 25 Ramadan 1439, corresponding to 10 June 2018, relating to the protection of natural persons in the processing of personal data, published in the JORA n ° 34 of 2018.
- Law no 25-11 of 28 Moharram 1447 corresponding to 24 July 2025 amending and supplementing law no 18-07 of 25 Ramadan 1439 corresponding to 10 June 2018 relating to the protection of natural persons in the processing of personal data, published in the JORA n ° 48 of 24 July 2025.

5. Reports:

- AI Council, *"Driving Innovation in AI for a Smarter Algeria"*, available on the website: www.aicouncil.dz accessed 26 Nov 2025.

6. Auther documents:

- General Data Protection Regulation (GDPR), regulation number 2016/679 of the European Parliament and of the Council of 27 April 2016, official journal of the European Union, 4 May 2016.
- UNESCO, *"recommendation on the ethics of artificial intelligence"*, 2021, available on the website: www.unesdoc.unesco.org