RESEARCH ARTICLE

Cybersecurity as a Legal and Social Pillar for Protecting Digital Rights and Enhancing Trust in the Digital Space

Mansouri Touria

Doctor (PhD)

Member of the Public Utilities and Development Laboratory, Djilali Al-Yabis University - Sidi Bel Abbes

Algeria

Email: mansouritouria1@gmail.com

Doi Serial https://doi.org/10.56334/sei/8.6.28

Keywords Digital Trust, Data Protection, Privacy Rights, Cyber Threats, Cyber security, Legal Frame works.

Abstract

Cybersecurity constitutes a fundamental pillar within the legal and regulatory framework aimed at safeguarding digital rights, foremost among them the right to privacy and the protection of personal data. In light of the accelerating digital transformation and the increasing reliance of economic actors and public authorities on digital systems for the collection and processing of data, it has become imperative to enact advanced legislation that ensures a delicate balance between the freedom of use and the legal protection of individuals against unauthorized or unlawful handling of their personal information.

In this context, cybersecurity can no longer be confined to its purely technical dimension. It now represents a multifaceted legal and societal responsibility that lies at the heart of restoring legal trust in the digital realm. The current challenges particularly the proliferation of cyber threats and attacks targeting information infrastructure necessitate the establishment of robust national and international cybersecurity policies. These must be underpinned by a clear, transparent, and multi-layered legal framework that guarantees fairness in digital data processing and reinforces the principles of transparency, accountability, and trust in electronic interactions.

Citation

Mansouri T. (2025). Cybersecurity as a Legal and Social Pillar for Protecting Digital Rights and Enhancing Trust in the Digital Space. *Science, Education and Innovations in the Context of Modern Problems*, 8(6), 263-275; doi:10.56352/sei/8.6.28. https://imcra-az.org/archive/364-science-education-and-innovations-in-the-context-of-modern-problems-issue-6-volviii-2025.html

Received: 11.01.2025 | Accepted: 27.04.2025 | Published: 15.05.2025 (available online)

Introduction

The digital sphere is undergoing rapid transformations that have redefined the boundaries of traditional freedoms and introduced unprecedented challenges for legal systems. These challenges revolve around how to reconcile the imperatives of security with the need to uphold fundamental rights and freedoms. In an era marked by escalating cyber threats and widespread digital practices that infringe upon personal data and freedom of expression, cybersecurity has emerged as a central theme in contemporary legal discourse not merely as a technical safeguard, but as a foundational element in rebuilding trust within the digital realm.

Recurrent cyberattacks and the growing threat of digital terrorism targeting critical infrastructure have compelled states to adopt increasingly stringent security policies, often justified by the necessity of preserving public order. However, such measures have expanded the scope of digital content surveillance and led to restrictions on key freedoms, particularly the right to privacy and freedom of expression. Still, this security-driven orientation must not be pursued in isolation from the principles of legality, proportionality, non-discrimination, and effective judicial

oversight. These safeguards are essential to prevent the digital space from becoming void of rights and freedoms.

From this perspective, cybersecurity represents a vital legal entry point for redefining the relationship between individuals and the state in the digital era, thereby fostering citizens' trust in the justice and transparency of the legal system. Legal trust is not merely built by shielding systems from cyber breaches; it is consolidated through the entrenchment of constitutional guarantees that ensure a fair balance between legitimate oversight and the protection of digital liberties.

This study, therefore, raises the following central research question:

To what extent can cybersecurity serve as a legal instrument for rebuilding trust in the digital space, in light of the inherent tension between surveillance imperatives and the protection of digital rights, particularly freedom of expression and the right to privacy?

To address this question, the study is structured around two primary axes:

- **Chapter One:** Freedom in the digital space and its legal boundaries
- **Chapter Tow:** Digital surveillance and cybersecurity as foundations for rebuilding legal trust

To examine the delicate balance between liberty and control in the digital realm and its implications for legal trust, this research adopts a descriptive-analytical method. It explores the concept of digital freedom, its unique legal features, and how it diverges from traditional freedoms, with a focus on the challenges posed by the evolving digital communication environment. It also delves into the notion of cybersecurity and the technical and regulatory frameworks developed by the Algerian legislator to combat cyber threats and deter perpetrators, in light of recent legal reforms.

In addition, the study employs an inductive approach by analyzing a selection of relevant national legal texts, aiming to identify prevailing legislative trends and assess their effectiveness in achieving a sustainable balance between digital security imperatives and the protection of fundamental rights and freedoms chief among them freedom of expression and the right to privacy in the digital environment.

Chapter One: Freedom in the Digital Space and Its Legal Boundaries

Throughout history, philosophers have emphasized the role of reason in mastering desire, even in the face of natural determinism. Simone Weil, in particular, articulated this idea with clarity, arguing that while human beings are bound by necessity, they nonetheless possess an inner freedom in how they respond to it. The essential distinction between slavery and freedom lies in the ability to choose: either to submit blindly to necessity or to engage with it through conscious and deliberate reflection.

The paradox highlighted by Weil is that rational thought traditionally regarded as the instrument of human liberation can, in the modern era, become a mechanism of domination through its technological manifestations, particularly artificial intelligence. In this sense, reason itself, once the symbol of emancipation, may transform into a threat to human freedom in the age of intelligent machines.[1]

The first requirement: The Legal Nature of Digital Freedom

Legal institutions and governing bodies endeavor to regulate digital freedom by establishing normative frameworks that govern its use and seek to prevent its slide into new forms of control or exclusion. However, this regulatory impulse often precedes a comprehensive understanding of the phenomenon itself. As a result, legal responses are frequently crafted hastily, lacking in-depth engagement with the inherent complexities of digital environments.

This reality renders digital freedom a fertile ground for rethinking the very notion of legal responsibility now caught between the poles of human autonomy and algorithmic governance. The tension between individual agency and automated control calls into question traditional legal categories and invites a reexamination of accountability in a landscape increasingly shaped by algorithmic decision-making.[2]

First branch: Freedom of Expression and Digital Privacy in International Instruments and National Legislation

In the context of rapid digital transformation, digital freedom has emerged as a subject of profound importance, sparking international debates that go far beyond

[1] **Patrick Pharo**, Nouveaux chemins de liberté, Les data contre la liberté, Hors collection 2022 Presses ? Universitaires de France, 2022, Pages 183-184.

[2] **Christian Byk et Daniela Piana**, L'intelligence artificielle : un « concept flottant » entre apparence de consensus normatif et controverse cachée sur le projet de société, Santé et intelligence artificielle Quelle(s) révolution(s) ? Droit, Santé et Société 2021/3 N° 3 ESKA, 2012, p 78-79-80.

technological considerations to touch upon deep cultural and anthropological differences in the understanding of freedoms across societies. Among the most prominent manifestations of this shift is artificial intelligence, which poses novel challenges to traditional conceptions of liberty and reshapes the relationship between the individual, the institution, and the law.

This evolving landscape calls for a comprehensive legal reading of digital freedom-one that acknowledges the interplay between ethical, social, and technological dimensions. Digital freedom can no longer be viewed merely as a right to access or express; rather, it is increasingly linked to new forms of responsibility that arise in an environment shaped by automation and algorithmic decision-making.

Thus, there is a growing need to reconceptualize freedom not solely as an abstract legal entitlement, but as a dynamic concept embedded within a technological system that reshapes reality and reorients human will. As philosopher Bernard Stiegler insightfully observes, technology today is no longer a passive tool at humanity's disposal it is generative of possibility itself. It does not simply enable what we imagine; it actively configures the very horizon of our imagination from the outset.

Firstly: At the International Level

In late 2001, Budapest witnessed the adoption of the first multilateral international treaty aimed at combating cybercrime - **the Budapest Convention on Cybercrime** - which was opened for signature on **23 November 2001** under the auspices of the Council of Europe. The Convention seeks to harmonize national criminal laws,[3] strengthen investigative techniques, and foster international cooperation in the fight against information-related crimes.

Its core objective is to establish a unified legal framework that enables signatory states to define cyber offenses, adopt appropriate sanctions, and align their domestic laws with common standards. One of the landmark accessions was that of the **United States**, which ratified the Convention in **September 2011**, thereby acknowledging its legal value in providing clear definitions of cybercrimes and facilitating cross-border enforcement.[4]

The **Budapest Convention**, in its Article 2 and subsequent articles, precisely defines crimes that infringe upon the confidentiality and security of information. It criminalizes **unauthorized access** to computer systems without legal permission. Article 3 also criminalizes the **illegal interception** of data transmissions using technical means with the intent to disrupt broadcasting or communication. It further includes **unauthorized interference with data**, such as intentional destruction, alteration, deletion, or corruption of digital data without lawful justification, considering such acts as criminal offenses subject to liability.

On the other hand, the **Council of Europe Convention on Cybercrime** highlights the member states' awareness of the growing and rapidly evolving threats posed by cybercrimes across computer networks. Its preamble emphasizes the urgency of adopting a unified criminal policy aimed at protecting society from these threats, through appropriate legislation and the strengthening of international cooperation. The Convention also underlines the profound transformations resulting from digitization and the globalization of networks, along with the increased potential for these networks to be used in the commission of complex criminal offenses.[5]

In order to protect commercial activities and deter crimes committed through electronic means, the Convention emphasized the necessity for State Parties to adopt legislative and other appropriate measures whenever required, to ensure the lawful and proper functioning of computer systems and the activities conducted through them.[6]

Secondly: At the Arab Regional Level.

The Arab region has undertaken concerted and structured efforts to strengthen cybersecurity frameworks. A key actor in this domain is the *Arab Center for Legal and Judicial Research*, which played a pivotal role in establishing the *Arab Observatory for Cybersecurity*, in collaboration with both governmental entities and civil society organizations. These initiatives culminated in the organization of the *Arab Cybersecurity Day* in Beirut-an event that underscored the imperative of aligning national legal systems across the Arab world with the evolving demands of modern digital technologies.

The forum emphasized the critical importance of legal harmonization and cooperative regulatory approaches in confronting cybersecurity threats and ensuring the resilience of digital infrastructure. It called for the integration of best legislative practices across the region and

[3] **Radia Lallouche**, *The Security of Electronic Signatures*, Master's thesis in Law, International Business Law Program, Department of Law, Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, 2012, pp. 169–170.
[4] **Radia Lallouche**,op, cit,p 170.
[5] http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm on **October 23, 2024, at 11:50 PM**.
[6] **Radia Lallouche**, op, cit, p 174.

advocated for the establishment of specialized regulatory bodies dedicated to the protection of personal and institutional data. Furthermore, a comprehensive public awareness campaign was launched during the event, aiming to enhance societal understanding of cybersecurity risks and the urgent need for both legal and technical safeguards.[7]

Third: At the National Level

The Algerian legislator has endeavored to establish a comprehensive legal framework to address the challenges related to the recognition and evidentiary value of electronic means of proof, with the aim of strengthening trust and security in digital transactions. In doing so, Algeria drew inspiration from international experiences, particularly the UNCITRAL Model Law. Various terminologies have been adopted to define cybercrimes, most notably "offenses against automated data processing systems" and "crimes related to information and communication technologies," as stipulated by Law No. 09-04.[8] This diversity in terminology reflects a multifaceted legislative approach.

Law No. 15-04 laid down foundational principles concerning documentation, integrity, and non-repudiation in the context of electronic signatures and authentication, while also criminalizing certain forms of digital forgery. These include, for instance, the submission of false information or the unauthorized use of another person's electronic signature. The law further emphasized the criminalization of acts that facilitate forgery, such as unauthorized access to information systems, as well as tampering with data that holds judicial evidentiary value.[9] Nevertheless, the current legal treatment of digital forgery remains partial and calls for a more comprehensive legislative enhancement to encompass all emerging forms and modalities of such crimes.

It is also worth noting that the confidentiality of information and personal data of digital environment users has been a primary concern across all sectors. This issue prompted the *International Organization for Standardization (ISO)* to pay particular attention to the matter, recognizing confidentiality as the principal reason for the development of encryption systems-given that it fundamentally concerns the ethics of online interactions.

Second section: The Limits of Digital Freedom Between Liberation and Restriction Amid Security Challenges

Digital freedom is not merely the ability to access or express oneself within the digital sphere; it is intrinsically linked to the **technical conditions** that determine what can be done or even thought of in the first place. What we often regard as free will in the use of digital tools is, in reality, preceded by a technological infrastructure that governs the nature of our choices and sets the boundaries of what is possible and impossible.

In this context, digital freedom cannot be understood outside its relationship with technology, which functions both as a precondition and a constraint on digital practices. Our projects and desires-those we perceive as outcomes of autonomous decisions-may in fact reflect opportunities and tools pre-determined by technological systems. Thus, the digital sphere becomes a contested space where individual will collide with the logic of automation and pre-programmed systems.

Herein lies the legal challenge: **How can we legislate for a genuine form of digital freedom that preserves an individual's capacity to choose within a space whose boundaries are technologically defined before they are consciously perceived?**

Recovering the legal meaning of digital freedom is not solely a matter of **data protection** or ensuring the **right to connectivity**; it requires a deeper interrogation of the very **technological foundations** that produce and simultaneously restrict freedom. In this sense, freedom is not only about "what we are allowed to do," but fundamentally about "**what we are allowed to imagine as possible.**"[10]

The second requirement: Challenges of Digital Freedom in Practical Reality

Amid the digital revolution that promised smarter cities and more personalized, efficient services, a fundamental paradox has emerged-one that strikes at the heart of the

[7] **Radia Lallouche**, op, cit, p 176.

[8] **Law No. 09-04** of 14 Sha'ban 1430 (corresponding to August 5, 2009), on the specific rules for the prevention and fight against crimes related to information and communication technologies, published in the Official Gazette No. 47 dated August 16, 2009. It was defined in Article 1 as: "Offenses affecting automated data processing systems as specified in the Penal Code, as well as any other offense committed or facilitated through an information system or electronic communication networks."

[9] In addition, the Algerian legislator, under Law No. 15-03 concerning the modernization of justice, criminalizes any act committed unlawfully by a person who uses elements related to the creation of an electronic signature linked to another person's signature. Accordingly, and based on these two legal texts, the electronic signature in question is technically valid and has not been altered; however, it was used by an unauthorized individual who signed in another's name, which constitutes forgery.

[10] **Bruno Bachimont**, Image et audiovisuel : la documentation entre technique et interpretation, Image et audiovisuel Documentaliste-Sciences de l'Information 2005/6 Vol. 42 A.D.B.S, 2005, 348.

very concept of digital freedom. Although digitization pledges to enhance daily life and empower individuals to interact instantly with services-whether in health, mobility, or urban management—the practical reality of these transformations reveals profound challenges to individual liberties, particularly the **freedom of movement**, **digital agency**, and the **right to privacy**.

At the core of these challenges lies the **collection and processing of personal data**, a process that has become central to every digital infrastructure. While necessary for tailoring services and improving efficiency, such data practices can lead to privacy violations and the creation of **"digital bubbles"**, which confine individuals within predetermined digital trajectories, thus restricting their autonomy and freedom of interaction.

In this context, digital freedom shifts from a theoretical concept to a **problematic field of application**, raising pressing questions:

- To what extent can access to smart services be considered true freedom, if such access is monitored and conditional?
- Do algorithms genuinely enable choice, or do they predefine it?
- What are the limits of balance between preventive measures (in health or behavior) and individual autonomy?

The French legislator was early to recognize these issues, enacting the **Informatics and Liberties Law of 1978**,[11] which emphasized that technology must serve humanity, not control it. Yet, four decades later, with the rise of tracking technologies and artificial intelligence, it has become clear that **ensuring digital freedom requires more than legal texts**. It must be embodied in **practical policies** that uphold **digital dignity** and restore individuals' control over their **personal data** and **digital pathways**.[12]

First branch: Unregulated Digital Practices and Their Impact on Public Order-A Comparative Perspective

The evolution of public administration under the framework of e-government represents a fundamental transformation in the administrative landscape. The incorporation of **digital mechanisms**, including automation, cloud computing, and data-driven services, has redefined power structures and operational dynamics within public institutions. While these advances promise efficiency, transparency, and accessibility, they have also paved the way-**in the absence of robust legal safeguards**-for the rise of **unregulated digital practices** that challenge the core principles of **public order**.

Notably, the **proliferation of open data initiatives** and the **deployment of artificial intelligence (AI)** in administrative decision-making, without clear legal parameters, have generated new forms of risk:

- **Administrative accountability** becomes blurred, as decisions are increasingly delegated to opaque algorithmic systems.
- **The principle of equality** is jeopardized when automated systems replicate or reinforce bias.
- **Privacy violations** become widespread in the absence of consent mechanisms and data minimization strategies.
- **Public trust in institutions** erodes due to perceptions of surveillance, lack of transparency, and the commodification of personal data.[13]

European Union Example: The GDPR and Digital Governance

The European Union has recognized these challenges and responded with the **General Data Protection Regulation (GDPR)**, a comprehensive legal framework that governs the collection, processing, and storage of personal data. The GDPR enshrines key principles that are essential for maintaining public order in digital governance:

- **Lawfulness, fairness, and transparency** in data handling (Article 5).
- **Purpose limitation and data minimization**, preventing excessive data collection.
- **Data subject rights**, including access, rectification, erasure, and objection.
- **Accountability obligations** for controllers and processors, including Data Protection Impact Assessments (DPIAs) for high-risk processing.[14]

[11] **Loi n° 78-17** du **6** janvier **1978** relative à l'informatique, aux fichiers et aux libertés. Article 1 : L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

[12] **Régis Chatellier**, Préserver notre liberté d'aller et venir dans le monde numérique, La liberté d'aller et venir dans le soin et l'accompagnement Sous la direction de Aurélien Dutier et Miguel Jean Regards croisés 2022 Presses de l'EHESP, 2022, p333.

[13] **David Brown,** Le gouvernement électronique et l'administration publique, 75ème anniversaire de l'Institut International des Sciences Administratives Revue Internationale des Sciences Administratives 2005/2 Vol. 71 I.I.S.A, 2005, p255-256.

This regulation is further supported by the **EU Digital Services Act (DSA)** and **Digital Governance Act**, which aim to impose greater responsibility on public and private entities using digital infrastructures, especially in domains like AI-based public services and cross-border data sharing.[15]

The Algerian Context: Toward Balanced Digital Governance

In Algeria, the absence of a **fully harmonized legal framework** for digital transformation in public administration has allowed digital practices to develop in a largely unregulated environment. The use of AI in administrative services, the sharing of open data without strict guidelines, and the implementation of e-services without embedded rights-protection frameworks contribute to structural risks:

- Inequitable access to services.
- Diminished legal recourse for automated administrative decisions.
- Threats to individual dignity and personal data autonomy.

The **digital transformation of governance** must be anchored in a normative framework that ensures **legal legitimacy**, **proportionality**, and **human-centered design**. Algeria and other states should:[16]

1. Adopt **comprehensive data protection laws** aligned with international best practices (e.g., GDPR).
2. Develop **AI governance policies** that promote transparency and human oversight.
3. Ensure **institutional accountability** in digital service provision.
4. Establish **independent regulatory authorities** with the capacity to enforce compliance and protect digital rights.

This balanced approach allows for the realization of technological benefits while preserving the foundational values of **equality**, **justice**, and **public order** in an increasingly digital society.

Second section: The Failure of Traditional Frameworks to Safeguard Individuals' Digital Rights

The digital transformation of public administration has fundamentally altered the relationship between the state and the citizen, rendering the regulation of information a critical legal imperative. However, digital advancements have exposed the shortcomings of traditional legal frameworks in protecting privacy and data security.[17] Paper-based laws are no longer adequate to address the complexities of the digital environment, thereby imposing new legal burdens on citizens without providing corresponding safeguards. The absence of effective protection for sensitive data threatens fundamental rights and undermines trust in state institutions, necessitating a comprehensive legal reform.

It may be asserted that smart cities suffer from a delay in implementing robust security strategies, due in part to the limited digital literacy of decision-makers, reliance on outdated technologies, and sluggish responsiveness to evolving cyber threats.[18]

Accordingly, the profound transformations brought about by e-government in the structure of public administration reveal that traditional legal and administrative frameworks are no longer sufficient to meet current - let alone future- digital challenges. As information technologies evolve and become deeply embedded in public service delivery, the protection of digital rights - such as privacy, freedom of access to information, and data security - can no longer be treated merely as extensions of classical legal norms. Rather, they require a fundamental reconfiguration of the concepts of governance, responsibility, and transparency.

While e-government does not constitute a transient phase but rather a structural transformation, the absence of a robust theoretical foundation and interdisciplinary approaches renders the formulation of an effective legal framework an urgent and complex challenge.

Thus, the development of digital infrastructure alone is insufficient. There is a pressing need to reform legal and administrative systems to ensure the protection of digital rights, and to strike a balance between administrative efficiency and the preservation of digital dignity in a constantly evolving digital landscape.

[14] **Dodds, T, Chengyuan,** L, Old Wine in New Bottles: Regulatory Approaches to Generative AI, Cadre européen incluant le RGPD et le DSA,2025, p 6.

[15] **Soderlund. Kasia**, AI Transparenceyin Trustworthy AI from Metaphor to Governance Tool in EU Technologiy Regulation, Faculty of Engineering, LTH. Land University, 2025, p 38-48.

[16] **Zerdoudi, A, Kouadria, M**, Analytical Study of Digital Transformation and Knowledge Economy in Arab Countries: Insights from the 2021 Reports, 2024, p14-18.

[17] **David Brown,** op, cit, p257.

[18] **Claudine Guerrier**, Cyber sécurité et entreprises de villes intelligentes, Smart cities et nouvelles formes d'entreprises Par Philippe Cohard et Pierre-Emmanuel Mérand Management des technologies organisationnelles 2020/1 N° 10 Les Presses des Mines, 2020, p 165-166-167.

Chapter tow: Digital Oversight and Cybersecurity as Foundations for Rebuilding Legal Trust

The escalating frequency and complexity of cyber threats[19] have given rise to a new digital reality that has profoundly shaken the foundations of trust in cyberspace. This evolving landscape has reignited fundamental questions concerning the capacity of states and institutions to safeguard digital rights. Within this context, digital oversight and cybersecurity have emerged as indispensable components-not only for protecting data-but also for reconstructing legal trust in the relationship between individuals and digital systems, both public and private. Cyberattacks targeting critical infrastructure or exploiting social networks, as well as health and financial data, underscore the fragility of conventional frameworks in securing the informational domain.

Thus, cybersecurity must be understood not merely as a set of technical tools, but as an integrated legal and regulatory governance structure essential for ensuring the availability, confidentiality, and integrity of data. This approach fortifies the rule of law within the digital sphere. The development of legitimate and transparent digital oversight mechanisms-grounded in principles of protection, accountability, and responsibility-is a decisive prerequisite for restoring citizen and institutional trust. Furthermore, it establishes a sustainable legal security environment that is capable of adapting to rapid technological transformations.[20]

Amid the escalating surge in cyber threats,[21] the French legislator has undertaken a series of legal measures aimed at confronting these challenges through an expanding legislative arsenal. This includes specialized laws such as the Informatique et Libertés Act of 1978.[22] and the Godfrain Law of 1988,[23] as well as the adaptation of traditional criminal offenses to the digital context. However, the recurrent nature of cyberattacks-particularly those targeting critical infrastructure-has revealed the limitations of conventional legal frameworks. This has necessitated the development of modern digital oversight mechanisms and the expansion of the cybersecurity concept to constitute an integral component of national sovereignty.

The first requirement: Cyber Oversight Between Security Protection and the Threat to Liberties.

Cybersecurity, in this context, represents not merely a collection of technical measures-as previously noted-but a comprehensive legal and institutional framework designed to restore trust between the citizen and the digital state. It aims to enhance the state's capacity to safeguard both individual and collective rights within the virtual domain. The reinforcement of this trust inevitably requires multi-level cyber governance, encompassing coordination between public and private sectors, reform of digital education, and the promotion of widespread awareness regarding cyber risks. Such efforts are essential for fostering a sustainable digital legal culture grounded in principles of responsibility, prevention, and institutional integration.

Thus, rebuilding legal trust in the digital age cannot be achieved without recognizing cybersecurity and digital oversight as instruments of sovereignty, essential for the protection of fundamental rights and the preservation of public order in the networked society.

First branch: Towards an Effective Deterrence Strategy in Compliance with International Law.

[19] In this regard, studies such as those by Fantin, Trouchoud, Ben Jabbour, and Gélin have revealed a concerning increase in cyberattacks—rising by 140% between 2013 and 2016—making smart cities constantly vulnerable to threats that cannot be addressed using traditional methods. The ISO/IEC 27032 standard aims to provide a comprehensive framework to confront such threats; however, its high implementation costs hinder widespread adoption, despite ongoing calls for the application of **Privacy by Design**, as stipulated in the European General Data Protection Regulation (GDPR).

[20] **David Brown,** op, cit, p260.

[21]The world's perception of the Internet has shifted from being a free and democratic space to a real arena of digital conflict, as a result of the rise in organized cyberattacks that have exposed the fragility of this domain. Pivotal events—such as the Estonia cyberattacks in 2007, the cyber conflict during the Russo-Georgian war in 2008, and the emergence of the Stuxnet virus that targeted Iranian nuclear facilities in 2009—marked key turning points in this transformation. These developments gave rise to new concepts such as "cyber weaponry" and "digital blockade," and the cyber domain has since been officially classified as the "fifth domain of conflict" in national defense strategies, alongside land, sea, air, and space.

[22] La **loi nu 78/17**, Modifié par Ordonnance **n°2018-1125** du **12** décembre **2018**. Article 1 : L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

[23] Loi Godfrain (1988), **Loi n° 88-19** du *5* janvier **1988** relative à la fraude informatique.

In this regard, this law was introduced at a time when information systems were gradually spreading within public administration and businesses. It provided a legal framework to address actions not covered by traditional laws, such as cyber piracy, and was considered a foundational reference for understanding digital sovereignty and cybersecurity in France and Europe.

The principle of coordinated and graduated deterrence has emerged as a foundational concept in shaping state responses to cyber threats. This approach advocates for a tiered classification system for cyberattacks that aligns with both domestic and international legal frameworks most notably Article 51 of the United Nations Charter, which serves as a legal basis for determining the appropriate forms of response, whether political, economic, diplomatic, or, in extreme cases, military. Harmonization between this classification system and that of strategic allies, such as the United States, opens the possibility for coordinated collective responses within international coalitions.[24]

This evolving legal landscape raises critical questions: When does a cyberattack constitute an "armed attack"? And does such an attack justify the invocation of the right to self-defense under Article 51? These uncertainties underscore the urgent need for enhanced international cooperation and the modernization of international legal instruments to encompass emerging domains such as digital sovereignty, cybercrime, and human rights in cyberspace.

At the international level, France's official point of contact for cyber incident monitoring and response is the CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), which operates under the authority of ANSSI (Agence nationale de la sécurité des systèmes d'information).[25] In addition, Article 7 of the Council of Europe Convention on Cybercrime recognizes cyber offenses as intentional unlawful acts, including the unauthorized provision of software, insertion of additional data, or the alteration, modification, or deletion of computer information without legal authorization.[26]

Second section: Cybersecurity Trends and Their Impact on the Right to Privacy.

In recent decades, the relationship between digital security and the protection of private life has undergone a profound transformation. This shift is largely attributed to the increasing complexity of cyber threats particularly those related to terrorism, organized crime, and the growing surveillance capabilities of states in the digital realm.

Firstly. From Data Protection to the Expansion of Surveillance Powers

During the 1980s and 1990s, initial efforts emerged to adapt legal frameworks to the realities of the emerging "information society." In 1986, the U.S. Congress amended the Electronic Communications Privacy Act (ECPA) to extend protections to digital files and email communications. Similarly, in 1995, the European Union adopted the Data Protection Directive, aiming to reconcile privacy protection with the free flow of data within the internal market.

However, this protective trajectory was paralleled by a growing body of legislation that expanded the surveillance and data interception powers of intelligence and law enforcement agencies-especially in the aftermath of the September 11, 2001 terrorist attacks. These events prompted the enactment of laws such as the USA PATRIOT Act, which significantly broadened investigative powers on the premise that counterterrorism imperatives could justify restrictions on civil liberties.

Secondly. Security vs. Privacy: The Rise of the "Securitization" of Cyberspace

A distinct trend toward the "securitization" of the digital domain has emerged-whereby technological challenges are increasingly framed as existential threats, justifying extraordinary security measures. This dynamic became particularly evident in France following the 2015 terrorist attacks, which led to the prolongation of the state of emergency and the passage of legislation granting expansive surveillance powers to security agencies. Notably, the 2017 Counter-Terrorism Law integrated emergency measures into the ordinary legal framework, often at the expense of privacy safeguards and without sufficient judicial oversight.[27]

[24] **Louis Gautier**, Cyber : les enjeux pour la défense et la sécurité des Français, Cybersécurité : extension du domaine de la lutte Inde : une résistible ascension Politique étrangère 2018/2 Été Institut français des relations internationales, P 29.

[25] **Amandine Lévêque**, Données et intelligence artificielle : quels enjeux pour la cybersécurité des États ? Le règne des données Cahiers français, 2021/1 n°419, La Documentation française, 2019, p 78-79.

[26] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

[27] **Loi n° 2017-1510** du **30** octobre **2017** renforçant la sécurité intérieure et la lutte contre le terrorisme.
In this regard, some French courts (including the Council of State) upheld the law, while emphasizing the necessity of respecting constitutional safeguards.

Third. The Snowden Revelations and the Crisis of Public Trust

In 2013, Edward Snowden's disclosures revealed the extensive reach of global mass surveillance programs operated by the U.S. National Security Agency (NSA). These revelations triggered international backlash and a significant erosion of public trust in digital governance. The United States responded by adopting the USA FREEDOM Act (2015), which aimed to curb certain surveillance practices. Simultaneously, the United Nations initiated global efforts to promote the right to privacy in the digital age.

Despite these efforts, the balance between privacy and security remains precarious. Following each major terrorist incident, political discourse often reverts to a heightened security narrative, resulting in a recurring pattern in which security interests systematically override privacy protections.[28]

Section Three: The Role of the Judiciary in Safeguarding the Principle of Proportionality and Fundamental Rights.

The judiciary particularly the Court of Justice of the European Union (CJEU) has played a pivotal role in curbing excessive surveillance practices and reinforcing the principle of proportionality in data governance. Notable judicial interventions include:[29]

The annulment of the Data Retention Directive in 2014 on the grounds that it violated the principle of proportionality and failed to ensure adequate safeguards for privacy. The invalidation of the "Safe Harbor" agreement between the European Union and the United States in the landmark Schrems I judgment (2015), due to insufficient protection of EU citizens' data.

The rejection of provisions in the UK Investigatory Powers Act, which were deemed incompatible with EU law, particularly in relation to indiscriminate data collection.

As data collection becomes increasingly pervasive especially through partnerships between governments and major technology firms growing concerns have emerged regarding the use of predictive analytics and digital profiling for surveillance or discriminatory practices. The Chinese Social Credit System has become a prominent example raising global apprehensions about state-led data-driven control mechanisms.

In this evolving landscape, the judiciary has come to represent the final bastion for upholding the balance between national security imperatives and the protection of fundamental human rights. Given the expansion of security agencies' powers under new legislation, judicial oversight alongside an empowered civil society is expected to play an increasingly vital role in ensuring that security measures remain constrained within a legal framework that respects privacy, due process, and essential liberties.[30]

The second requirement: The Role of Modern Legislation in Ensuring an Effective Balance Between Oversight and Liberties (The Algerian Legal Framework as a Case Study).

Under the provisions of Law No. 09-04 of 5 August 2009, concerning the specific rules for the prevention and suppression of offenses related to information and communication technologies, Algeria established a national authority known as the National Authority for the Prevention of ICT-Related Crimes. This body functions as an independent administrative authority,[31] endowed with legal personality and financial autonomy, and is placed directly under the authority of the President of the Republic.[32]

First branch: The National Cybercrime Authority: A Centralized Oversight Structure Anchored in Presidential Accountability.

[28] In this context, major European countries—such as Germany, France, and the United Kingdom—have enacted laws aimed at enhancing their intelligence capabilities. These include the United Kingdom's *Investigatory Powers Act* (2016), Germany's *Communications Intelligence Gathering Act* (2016), and France's international surveillance law adopted following the 2015 attacks. These legislative frameworks permit extensive data collection, including from Internet Exchange Points (IXPs), and have sparked significant legal controversy concerning judicial oversight and the degree to which the principles of necessity and proportionality are upheld.

[29] **Marilia Maciel-Hibbard**, Protection des données personnelles et cyber(in)sécurité, Cybersécurité : extension du domaine de la lutte Inde : une résistible ascension Politique étrangère 2018/2 Été Institut français des relations internationales, P 63-64

[30] **Marilia Maciel-Hibbard,** op, cit, P 65.

[31] **Presidential Decree No. 19-172 of June 6, 2019**, setting the composition, organization, and functioning modalities of the **National Body for the Prevention and Fight against Information and Communication Technology-related Crimes**, published in the **Official Gazette No. 37, dated June 9, 2019**.This decree was **amended and supplemented by Presidential Decree No. 21-439 of November 7, 2021**, concerning the reorganization of the same national body, and published in **Official Gazette No. 86, dated November 11, 2021**.

[32] **Article 2 of Presidential Decree No. 20-183 of July 13, 2020**, concerning the reorganization of the **National Body for the Prevention and Fight against Information and Communication Technology-related Crimes**, published in the **Official Gazette No. 40, dated July 18, 2020**.

The organization and composition of the Authority are determined by regulatory instruments, while its official headquarters is located in Algiers, with the possibility of relocation anywhere within the national territory by presidential decree. The Authority is structured into two main subdivisions: The Guidance Council and the General Directorate,[33] both of which report directly to the President and are required to submit periodic activity reports to the Head of State.

This institutional design reflects a legislative intent to integrate cybersecurity oversight within a framework of centralized accountability, while aiming to strike a balance between the imperatives of digital crime prevention and the respect for civil liberties. As such, this model offers a notable example of how modern legal mechanisms can institutionalize digital oversight while remaining anchored in a constitutional order.[34]

The National Authority for the Prevention of Crimes Related to Information and Communication Technologies is entrusted, within the framework of its legal duties, with promoting and coordinating preventive measures against this type of crime. It exercises a set of key prerogatives that enable it to fulfill its objectives, which include:

- Proposing legislative and regulatory policies and mechanisms aimed at enhancing the protection of society from cyber threats.
- Promoting and coordinating operations for the prevention of ICT-related crimes.
- Assisting the judiciary and law enforcement officers in the fight against cybercrime, particularly regarding the gathering and provision of information.[35]
- Ensuring preventive monitoring of electronic communications to detect crimes of a terrorist nature or those threatening state security, in coordination with the Ministry of Defense when matters relate to military security, and in accordance with applicable legislation.[36]
- Contributing to the training of specialized investigators in technical investigations related to information and communication technologies.[37]
- Additionally, the Authority is tasked with recording and preserving digital data from information systems and identifying their source and trajectory for use in judicial proceedings.[38]

Accordingly, the initiative taken by the Algerian legislator to establish the National Authority for the Prevention of Cybercrime under Law No. 09-04 represents a positive and significant legislative step toward strengthening the institutional framework for preventing risks associated with the use of information and communication technologies.

However, despite its importance, this initiative alone remains insufficient to confront the growing and evolving challenges posed by cybercrime-particularly given the continuous advancement of the tools and methods used to commit such crimes in the digital environment. This reality necessitates a comprehensive and integrated approach, encompassing the reinforcement of the legislative framework, the development of technical competencies, and the activation of international cooperation mechanisms in this field.

Second section: Regulating the Digital Infrastructure: The Role of the Postal and Electronic Communications Authority in Cybersecurity

Similar to the National Authority for the Prevention of Crimes Related to Information and Communication Technologies, the Algerian legislator, under Law No. 18-04[39] of May 10, 2018, related to postal and electronic communications, established the Regulatory Authority for Postal and Electronic Communications as an independent administrative body with legal personality and financial autonomy.

This authority is tasked with ensuring compliance with regulatory rules applicable to operators in the postal and electronic communications sector. It is also entrusted with contributing to the achievement of cybersecurity,[40] through

[33] In addition, **Articles 6 to 8 and Articles 9 to 13 of Presidential Decree No. 21-439**, previously mentioned, further detail the structure and functioning of this national body.

[34] **Article 2 of Presidential Decree No. 20-183**, previously mentioned.

[35] **Article 14 of Law No. 09-04**, previously mentioned.

[36] **Article 4(4) of Presidential Decree No. 21-439**, previously mentioned.

[37] **Article 4(5) of Presidential Decree No. 21-439**, previously mentioned.

[38] **Article 4 of Presidential Decree No. 20-183**, previously mentioned.

[39] **Law No. 18-04 of 24 Sha'ban 1439 AH (corresponding to May 10, 2018)**, establishing the general rules relating to postal and electronic communications, published in **Official Gazette No. 27, dated May 13, 2018**.

[40] Cybersecurity has been defined in Article 10/03 of Law No. 18/04, which sets forth the general rules governing postal services

its role in combating cybercrimes and addressing the risks associated with the unlawful use of communication networks, in accordance with existing legislation.

Section Three: Law No. 18-07 on Data Protection: A Legal Guarantee for Privacy in the Digital Age.

In addition, the Algerian legislator introduced Law No. 18-07 of June 10, 2018, concerning the protection of natural persons in the context of automated processing of personal data. This legislative development represents a crucial step in enshrining the right to privacy and the protection of personal life within Algerian legislation, in line with digital and informational transformations. The law was enacted in response to international standards, particularly those found in human rights instruments and data protection agreements.

The objective of this law is to establish a comprehensive legal framework to regulate the collection, processing, storage, and transfer of personal data, while ensuring adherence to fundamental principles such as legality, transparency, and proportionality.

Furthermore, the law establishes a set of rights for individuals whose data is subject to processing, including the right to information, access, correction, deletion, and objection, and grants them the right to appeal to the National Authority for the Protection of Personal Data. This body, created by the same law, is an independent administrative authority with regulatory and supervisory powers.

The law obliges all parties involved in the automated processing of personal data to comply with data security rules and to obtain prior authorization from the Authority, especially in cases involving sensitive data or transfers of data abroad. It also introduces criminal and administrative penalties for anyone found guilty of illegal processing, disclosure, or use of data outside the declared purposes, reflecting the legislative seriousness in protecting this fundamental right.

Thus, Law No. 18-07[41] constitutes a modern reference framework within Algerian legislation for personal data governance in the digital economy era.

Conclusion:

Cybersecurity has become one of the fundamental pillars for ensuring state sovereignty and internal stability, particularly in light of the rapid shift toward digitization and the growing scale of cyber threats targeting critical infrastructure, sovereign data, and individual rights. In the Algerian context, an analysis of the current legal and institutional framework reveals a notable evolution in the legislative measures combating cybercrime, as reflected in Laws No. 09-04, 18-04, and 18-07. However, this legislative progress remains partial unless it is supported by a comprehensive strategic vision that strengthens national cyber resilience and keeps pace with the ongoing transformation of the digital landscape.

Based on the study conducted, a number of key findings have been reached, summarized as follows:

1. The Algerian legal framework has shown tangible progress in recognizing the seriousness of digital threats by establishing specialized bodies and clearly defining responsibilities for protecting data and combating cybercrime.

2. Existing legislation suffers from certain shortcomings, particularly in adapting legal texts to the evolving technical nature of cybercrime and in the lack of coordination among relevant entities.

3. The Algerian experience reveals an urgent need for a unified national cybersecurity strategy that overcomes the fragmented nature of current approaches.

4. Institutional capacity to address cross-border digital crimes remains limited, alongside weak levels of international cooperation in this domain.

5. There is a shortfall in the involvement of civil society and the private sector in prevention and response efforts, which hinders the achievement of collective digital resilience.

6. Legal oversight over the automated processing of personal data represents a qualitative advancement, yet it

and electronic communications (as previously mentioned), as: *"A set of tools, policies, security concepts, security mechanisms, guidelines, risk management approaches, operational procedures, training, best practices, safeguards, and technologies that may be employed to protect electronic communications against any incident that could compromise the availability, integrity, or confidentiality of data that is stored, processed, or transmitted.*

[41] **Law No. 18-07 of 25 Ramadan 1439 AH (corresponding to June 10, 2018)**, concerning the protection of natural persons in the processing of personal data, published in **Official Gazette No. 34, dated June 10, 2018.**

still requires stronger guarantees for the protection of rights and freedoms.

Recommendations:

1. Prioritize the protection of sovereign systems and critical infrastructure by reinforcing them both technically and legally, while developing a precise list of sensitive facilities requiring special protection.

2. Adopt a proactive and flexible cyber defense doctrine based on early detection capabilities, digital deterrence, and rapid response, all within clear legal frameworks that uphold constitutional standards and human rights.

3. Achieve full national digital sovereignty through the development of secure local systems for encryption, data storage, and computing, while reducing reliance on foreign technologies and infrastructures.

4. Build the capacity of the judiciary and investigative bodies in the field of cybercrime law, and modernize criminal procedures to align with the unique characteristics of digital crime.

5. Promote widespread public awareness of digital security through educational and media programs targeting all societal segments, thereby embedding cybersecurity into everyday practices of individuals and institutions.

6. Strengthen regional and European integration in combating cyber threats through the harmonization of legal and technical standards and the exchange of information and security expertise.

7. Advocate for a fair and responsible international governance model of cyberspace based on the principles of shared responsibility, respect for state sovereignty, and prevention of the militarization of the digital domain.

Sources and References

I. Sources and References in Arabic:

A / Legal Texts:

1. **Law No. 18-04 of 24 Sha'ban 1439 AH (corresponding to May 10, 2018)**, defining the general rules related to postal and electronic communications, *Official Gazette*, No. 27, published on May 13, 2018.
2. **Law No. 18-07 of 25 Ramadan 1439 AH (corresponding to June 10, 2018)**, on the protection of natural persons in the processing of personal data, *Official Gazette*, No. 34, published on June 10, 2018.
3. **Law No. 09-04 of 14 Sha'ban 1430 AH (corresponding to August 5, 2009)**, setting out special rules for the prevention and fight against crimes related to information and communication technologies, *Official Gazette*, No. 47, published on August 16, 2009.
4. **Law No. 15-03 of 11 Rabi' al-Thani 1436 AH (corresponding to February 1, 2015)**, concerning the modernization of justice, *Official Gazette*, No. 6, published on February 10, 2015.

B/ Presidential Decrees:

1. **Presidential Decree No. 19-172 of June 6, 2019**, specifying the composition, organization, and functioning modalities of the National Body for the Prevention and Fight against Information and Communication Technology-related Crimes, *Official Gazette*, No. 37, published on June 9, 2019, as amended and supplemented by **Presidential Decree No. 21-439 of November 7, 2021**, published in *Official Gazette* No. 86, dated November 11, 2021.
2. **Presidential Decree No. 20-183 of July 13, 2020**, reorganizing the National Body for the Prevention and Fight against Information and Communication Technology-related Crimes, *Official Gazette*, No. 40, published on July 18, 2020.

C/ Academic Articles :

1. **Radia Lallouche**, *The Security of Electronic Signatures*, Master's thesis in Law, International Business Law Program, Department of Law, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, 2012, pp. 169–170.

D / Electronic Sources:

http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm on **October 23, 2024, at 11:50 PM**

II. List of References and Sources (FRANCE):

A. Laws :

a) **Loi n° 78-17** du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La **loi nu 78/17**, Modifié par Ordonnance **n°2018-1125** du 12 décembre 2018.
b) Loi Godfrain (1988), **Loi n° 88-19** du *5* janvier 1988 relative à la fraude informatique.
c) **Loi n° 2017-1510** du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

B. Books :

1. Patrick Pharo, Nouveaux chemins de liberté, Les data contre la liberté, Hors collection 2022 Presses ? Universitaires de France, 2022.
2. Régis Chatellier, Préserver notre liberté d'aller et venir dans le monde numérique, La liberté d'aller et venir dans le soin et l'accompagnement Sous la direction de Aurélien Dutier et Miguel Jean Regards croisés 2022 Presses de l'EHESP, 2022.
3. Soderlund. Kasia, AI Transparenceyin Trustworthy AI from Metaphor to Governance Tool in EU Technologiy Regulation, Faculty of Engineering, LTH. Land University, 2025.
4. Dodds, T, Chengyuan, L, Old Wine in New Bottles: Regulatory Approaches to Generative AI, Cadre européen incluant le RGPD et le DSA,2025

C. Articles :

1. Amandine Lévêque, Données et intelligence artificielle : quels enjeux pour la cybersécurité des États ? Le règne des données Cahiers français, 2021/1 n°419, La Documentation française, 2019.
2. Bruno Bachimont, Image et audiovisuel : la documentation entre technique et interpretation, Image et audiovisuel Documentaliste-Sciences de l'Information 2005/6 Vol. 42 A.D.B.S, 2005.
3. Christian Byk et Daniela Piana, L'intelligence artificielle : un « concept flottant » entre apparence de consensus normatif et controverse cachée sur le projet de société, Santé et intelligence artificielle Quelle(s) révolution(s) ? Droit, Santé et Société 2021/3 N° 3 ESKA, 2012.
4. Claudine Guerrier, Cyber sécurité et entreprises de villes intelligentes, Smart cities et nouvelles formes d'entreprises Par Philippe Cohard et Pierre-Emmanuel Mérand Management des technologies organisationnelles 2020/1 N° 10 Les Presses des Mines, 2020.
5. David Brown, Le gouvernement électronique et l'administration publique, 75ème anniversaire de l'Institut International des Sciences Administratives Revue Internationale des Sciences Administratives 2005/2 Vol. 71 I.I.S.A, 2005.
6. Louis Gautier, Cyber : les enjeux pour la défense et la sécurité des Français, Cybersécurité : extension du domaine de la lutte Inde : une résistible ascension Politique étrangère 2018/2 Été Institut français des relations internationales.
7. Marilia Maciel-Hibbard, Protection des données personnelles et cyber(in)sécurité, Cybersécurité : extension du domaine de la lutte Inde : une résistible ascension Politique étrangère 2018/2 Été Institut français des relations internationales.
8. Zerdoudi, A, Kouadria, M, Analytical Study of Digital Transformation and Knowledge Economy in Arab Countries: Insights from the 2021 Reports, 2024.