

Digital Public Order

Dr. Souaad MEDJADJI

University of Aïn Témouchent, Algeria

Email : souad.medjadji@univ-temouchent.edu.dz

Received: 23/11/2025 ; Accepted : 09/05/2026 ; Published : 26/07/2026

Abstract:

The concept of public order (ordre public) constitutes a pivotal and vital subject in all legal systems, holding a prominent place across various branches of both public and private law. The notion of public order cannot be confined to a narrow scope, free from overlap or interplay with other concepts, as it remains a flexible doctrine that expands or contracts according to the prevailing circumstances of each society.

Furthermore, current technological advancements and the information revolution have brought the concept of public order face to face with the evolving challenges of the electronic era and the digital space, which operates on non-traditional fundamentals and distinct elements regarding spatial, temporal, personal, and factual boundaries. Consequently, adapting traditional mechanisms to preserve public order within this new digital environment has proved increasingly difficult.

Perhaps the greatest threat facing public order is its collision with the concept of digital freedom, as public authorities tasked with maintaining public order within society no longer find it easily feasible to assert control and oversight over this digital sphere. Additionally, globalization and digital connectivity—having erased geographical borders—have further compounded the complexities confronted by law enforcement authorities. In practice, the protection of public rights and freedoms does not always manifest uniformly across all times and places, even within a single state, and its regulatory patterns do not operate at a constant level; hence, the challenges are inherently magnified within cyberspace.

From this context emerges a new dimension of public order, namely **Digital Public Order**, aimed at confronting digital chaos. This paper addresses the problem of maintaining public order in the electronic realm, requiring first an examination of the legal foundations (doctrinal grounding) of the concept of digital public order, followed by an analysis of the extent to which existing legislation contributes to its framing and the determination of its core components.

Keywords: Cyberspace — Digital Rights and Freedoms — Public Order — Digital Sovereignty — Cybersecurity.

Introduction:

The digital space has become a vital element within the international system and in managing interactions among This development has been further catalyzed by the emergence of what is ¹. known as digital rights and freedoms. Despite the progress brought about by the digital revolution, it has also produced adverse effects that negatively impact societal order, often undermining the

¹ Magda Abdel Shafeek, Constitutional Protection of Cybersecurity and Its Impact on Public Order, Journal of Legal and Economic Research, Vol. 57, No. 4, Faculty of Law, Menoufia University, Egypt, p. 349. Available at: [http://Jslem.journals.ekb.eg.artic](http://Jslem.journals.ekb.eg.artichttp://Jslem.journals.ekb.eg.artic) Accessed: December 1, 2024, at 11:30 AM.

governing values upon which societies are founded. In the absence of appropriate regulatory frameworks, misuse can impede this progress; therefore, recent technical developments must be accompanied by legislative evolution aimed at mitigating all risks that threaten public order in both its traditional and modern senses.

In the digital era, public order has acquired a virtual dimension, requiring authorities to redefine their instruments and strategies to respond effectively to new technological challenges. Thus, the modern concept of public order becomes a synthesis of traditional measures and advanced techniques, integrating physical security, digital security, and information security simultaneously. All of this must be achieved while striking a balance between leveraging the digital revolution and its modern technologies, and satisfying the requirements of preserving public order without compromising digital rights. This occurs in light of scientific and technological advancements that have permitted ². the expansion of human rights into cyberspace, leading to the emergence of a new pattern of fourth-generation human rights associated with the freedom to use information and communication ³. technology tools, as well as freedom of expression ⁴.

The exercise of these rights in the virtual world or digital society imbues them with distinct characteristics and manifestations that differ from traditional rights. Furthermore, the absence of an ⁵. explicit constitutional framework for digital rights creates a legislative void that certain authorities may exploit to restrict digital freedoms. The threat of violating digital rights is not confined to governmental entities; it extends to private tech giants that collect personal data, direct content, and control social platforms ⁶.

Researching this topic assumes particular significance, especially given that the internet now anchors transactions across all fields, creating an interconnected world that no longer recognizes spatial or temporal boundaries. All these factors have reshaped practices and interactions among individuals, while many users overlook a critical aspect of the digital space known as cybersecurity—rendering them more vulnerable than ever to malicious attacks, infringements, fraud, and other undesirable occurrences. Consequently, there is an imperative need to re-establish public order within the digital space. As an effective mechanism to curb the autonomy of the will (*autonomie de la volonté*) and safeguard society's paramount interests, public order reflects the supremacy of the state's entity and asserts its stability against individual tendencies that threaten societal foundations. Moreover, it serves as an instrument in the hands of the state to prevent private wills from undermining the fundamental interests of society ⁷.

This research aims to establish key foundational pillars upon which the new digital public order relies. Amid attempts to reconcile the preservation of rights with regulation, the following core

² Roqaya Saeed Abdel Lateef Abdo, The Risks of Modern Electronic Means to the State's Public Order, The Legal Journal, Vol. 22, No. 9, Faculty of Law Khartoum Branch, Cairo University, Egypt, 2024, p. 3450.

³ Suzanne Lequette, Droit du numérique Digital Law, LGDJ, Lextenso, France, 2024, p. 132.

⁴ Ghania Ben Kroidem, Digital Rights: Reality and Challenges, Journal of Comparative Legal Studies, Vol. 7, No. 1, Hassiba Benbouali University of Chlef, 2020, p. 2035.

⁵ Larbi Derai, The Dialectic of Balancing the Exercise of Digital Rights and the Protection of Digital Sovereignty in Algerian Legislation, Journal of Human Rights and Public Freedoms, Vol. 11, No. 1, Faculty of Law and Political Science, Abdelhamid Mehri University of Mostaganem, 2026, p. 735.

⁶ Mohamed Sobhi Hassan Ali, Constitutional Protection of Digital Rights, International Journal of Jurisprudence, Judiciary, and Legislation, Vol. 6, No. 2, Egyptian Judges Club, 2025, p. 423.

⁷ Hussein Abdullah Al-Kelabi, Contractual Public Order L'ordre public contractuel, Al-Sanhouri Library, 1st ed., Beirut, Lebanon, 2016, p. 9.

research question arises: **Does the concept of public order effectively fulfill its designated role within the digital space?**

From this primary problem, the following sub-questions emerge:

- What are the methods and legal bases governing the intervention of public authorities alongside other legal systems or cultures within this new medium?
- How can the line of demarcation be drawn between the protection of public order and the rights of internet users?

Answering these questions is intrinsically linked to the impact of internet usage on public order (ordre public). This requires an examination of the methods and limits of public authority intervention regarding this medium when confronted with the private sphere of internet users. Furthermore, the global nature of the internet exposes the Algerian concept of public order to a supranational framework when intersecting with other legal systems or cultures, particularly given that domestic public order constitutes a legal phenomenon aimed at safeguarding the fundamental values and principles upon which society is established. Indeed, rules considered part of public order in a given state may not carry the same status in others.

The significance of this study lies in the fact that the concept of public order serves as one of the most prominent and powerful guarantees safeguarding societal interests. It functions as a shield against any agreement or act detrimental to the public interest or contrary to society's moral code and its potential negative repercussions, regardless of the individual interests secured by the parties involved. Faced with the growing threat to the concept of public order within society under the guise of digital freedom and the absence of clear liability boundaries in the digital space, it has become imperative to reconsider the requirements of public order and attempt to adapt them in light of this new reality.

Additionally, the importance of this subject is underscored by its address of the extent to which legal rules keep pace with societal developments, accommodate and regulate individual transactions, and highlight the obstacles arising from adapting legal texts to the unique characteristics of the digital realm.

This study relies on the descriptive and analytical methodologies, as they are the most suitable for the subject matter, in addition to the comparative approach through the examination of international experiences and the positioning of Algerian legislation among comparative legal systems regarding its coverage of the digital domain. Through this approach, we seek to identify the gaps in Algerian law in terms of mechanisms, vision, or strategic planning. To address the aforementioned problem, a two-part structure has been adopted, organized under the following titles:

Section I : The Concept of Digital Public Order

Section II: The Legal Framing of Digital Public Order

Section I: The Concept of Digital Public Order

Given the flexibility and ambiguity inherent in the notion of public order (ordre public), legal scholars and commentators have long sought to define it, yet without reaching a universally consensus-based or exhaustive definition (définition une et indivisible). Public order remains a broad and elastic concept whose practical applications in law are notably expansive and non-exhaustive⁸. Defining such dynamic legal notions presents inherent conceptual challenges. Accordingly, this

⁸ Allaq Abdelkader, The Problem of Defining the Concept of Public Order, Al-Mi'yar Journal, Vol. 10, No. 4, Tissemsilt University, December 2019, p. 4.

section examines the traditional concept of public order prior to analyzing how digital transformation has reshaped its core tenets.

A. The Traditional Concept of Public Order

The concept of public order stands as one of the most elusive legal constructs within legal doctrine (doctrine). Rather than offering an absolute definition, legal commentators have largely focused on illustrating its scope and characteristics. Historically, public order became deeply intertwined with the legal notion of public interest—a synergy that solidified alongside the emergence of social legal theory, which prioritizes collective interests over individual autonomy Public order⁹. is generally defined as a set of mandatory rules intended to achieve fundamental political, social, or economic interests concerning the overarching organization of society. Because these rules supersede private interests, all individuals are legally bound to observe them, and any private agreements in derogation thereof are null and void (nullité d'ordre public), as private convenience cannot prevail over public necessity¹⁰.

The conceptualization of public order varies significantly between public law and private law:

- **In Public Law:** Public law scholars define public order as the imperative baseline that administrative authorities are legally mandated to preserve through their core function of administrative policing (police administrative). This traditional triad encompasses public safety, public security, public health, and public tranquility¹¹.

- **In Private Law:** Jurists view public order as the foundational political, social, economic, and moral framework upon which the state is established, as articulated by positive law. Alternatively, it is understood as the body of imperative rules governing political, social, economic, or moral interests that directly concern the community at large rather than private individuals Ultimately, it¹². constitutes the essential interest matrix vital to maintaining societal cohesion, without which the stability of the state entity would be compromised.

Rules pertaining to public order are imperative (règles impératives / jus cogens); private autonomy (autonomie de la volonté) possesses no authority to bypass or violate them, as any contravention threatens the foundational structure of society with instability Furthermore, public¹³. order is inherently relative across time, space, and jurisdiction—what is deemed fundamental to public order in one society may not hold the same legal weight in another. It adapts dynamically to prevailing political, economic, and philosophical paradigms, which accounts for the multiplicity of doctrinal definitions.

In this context, the traditional notion of public order can expand or contract depending on prevailing societal trends, rendering its confinement to a rigid formula impractical due to its relative and evolutionary nature. Defining public order is further complicated by rapid socio-economic shifts and increasing state intervention across various sectors. This intervention has fragmented the unity

⁹ Allaq Abdelkader, Ibid., p. 3.

¹⁰ Abd El-Razzak El-Sanhuri, Al-Waseet in the New Civil Law: General Theory of Obligations - Sources of Obligation, Halabi Legal Publications, Beirut, Lebanon, 2000, pp. 399–400.

¹¹ Imad Tarek Al-Bishri, The Concept of Public Order in Theory and Practice: A Comparative Study Between Positive Laws and Islamic Jurisprudence, 1st ed., Al-Maktab Al-Islami, Beirut, Lebanon, 2005, p. 19.

¹² Milat Abdelhafid, The International Nature of the Internet and the Concept of Public Order: Determining Liability for Breaching Public Order in Contracts Relating to Web Hosting and Access Services, Image and Communication Journal, Vol. 5, No. 19, Laboratory of Mass Communication and Semiotics of Visual Systems, University of Oran, 2016, pp. 29–30.

¹³ Ahmed Abdelhamid Amin, The Role of the Concept of Public Order in Protecting Contractual Legality and the Weaker Party, Journal of the Faculty of Law, Vol. 2, No. 1, Part 1, Minia University, Egypt, June 2019, pp. 71–72.

of public order into distinct domain-specific regimes. Additionally, the legal system increasingly¹⁴ encounters novel legal transactions birthed by technological progress that outpace traditional legislation. In these instances, technology generates novel legal facts in the absence of explicit statutory or customary coverage. Because technological advancement is continuous, the law must similarly evolve to proactively address both the positive outcomes and negative externalities that inevitably challenge traditional legal principles.

B- The Impact of Digital Transformation on the Evolution of the Concept of Public Order

The world has witnessed a massive expansion in information technology, communications, and modern technological applications driven by the Fourth Industrial Revolution, which has asserted itself forcefully across numerous domains. This revolution rests upon three primary pillars: the Internet of Things (IoT), Big Data, and Artificial Intelligence (AI). Consequently, the law often finds itself unable to keep pace with this smart digital revolution. This state of affairs has reshaped numerous legal and human rights concepts, placing national legislators in a position where they struggle to regulate emerging legal situations—situations whose legitimacy they cannot deny, yet whose legal framework remains elusive¹⁵.

Insofar as a legal system serves as a mirror reflecting society's tendencies and drive toward targeted organization aimed at protecting individual and collective rights, as well as safeguarding institutions and legal positions across various statutory branches, it is natural that its philosophy, rules, and legislative foundations have been influenced by the digital space and the novel patterns of legal relations it has forged¹⁶.

In practice, the growing adoption of digital technologies destabilizes public order and security, as these technologies heighten the risk of disseminating illegal content—such as content inciting hatred, discrimination, or violence against children and minors, who are increasingly exposed to sensitive material that may adversely affect their psychological health and safety. Furthermore, the escalation of cybercrime poses another critical threat tied to the rise of digital technology. Digital advancement also introduces novel security and safety risks by fueling certain expressions of freedom of speech that are occasionally exploited to propagate insults, defamation, and disinformation.

The absence of law within the digital space directly conflicts with the preservation of rights and freedoms, just as lawlessness undermines public order itself. The ultimate goal is to transpose the public order existing in real life onto a digital scale. However, what is the current state of affairs regarding this new environment known as the digital space? And what becomes of state sovereignty in enforcing the law within an immaterial realm featuring blurred borders?

In attempting to trace the extension of public order into the digital sphere, we face a series of challenges—first and foremost regarding the physical meaning of the digital world. The technological evolution that flourished under the information revolution has given rise to a new generation of concepts, such as **globalization** (denoting the openness of the world's peoples to one another across

¹⁴ Philippe Malaurie, *La notion de l'ordre public et les bonnes mœurs en droit privé* The Concept of Public Order and Good Morals in Private Law, Report presented to the Henri Capitant Association for French Legal Culture, Vol. 7, 1950.

¹⁵ Mohamed Irfan Khateeb, *Guarantees of Rights in the Digital Era: From Changing Concepts to Evolving Protection — A Reading of the European and French Legislative Stance with Applications to Kuwaiti Legislation*, Kuwaiti Journal of Law, Special Supplement, Vol. 42, No. 3, Part 1, Academic Publication Council, Faculty of Law, Kuwait University, May 2018 Sha'ban 1439 AH, p. 253.

¹⁶ Ismail Ougadi, *Digital Space and the Need for a New Legal Paradigm*, Takamoul Center for Studies and Research, January 15, 2021, p. 5. Available at: <https://www.takamoul.org><https://www.takamoul.org> Accessed: May 12, 2026, at 11:00 AM.

all fields) and the **global village** (reflecting the compression of time and space, where the world appears as a small village unseparated by geographic boundaries or physical barriers) ¹⁷.

As a byproduct of this shift, a new dimension of public order has emerged: **Digital Public Order** which has come to symbolize the legal baseline and structural framework aimed at curbing digital ¹⁸ chaos. The new realities introduced by the digital revolution have rendered time and space relative to the extreme. This relativity severely impairs the enforcement of national rules intended to govern individual conduct within a specific, geographically defined territory under the principle of territoriality of laws (*principe de territorialité des lois*), as their application within an elusive, geographically boundless digital world proves exceptionally difficult.

From this perspective, spatial boundaries stand as a major impediment to enforcing legal texts that frame digital public order. Furthermore, the evolving concept of public order in the digital realm exposes another obstacle concerning the very foundation of the rules governing this virtual world—specifically, the political, social, economic, and moral benchmarks underpinning public order. The blending of diverse societies within the digital space makes it exceedingly difficult to agree upon a common set of universally accepted rules to govern all domains across the globe ¹⁹.

Section II : The Legal Framing of Digital Public Order

Law and order face unprecedented challenges given the rapid evolution of technology and its pervasive impact on society. In the absence of appropriate safeguards and regulatory frameworks, digital technology is prone to misuse. Real progress and innovation can only thrive under intelligent, responsible oversight; thus, the challenges confronting public order necessitate re-establishing **digital sovereignty** over the digital space and its various applications. Indeed, no public order can exist without digital sovereignty ²⁰.

States possess a range of instruments enabling them to reshape their national borders within cyberspace through practices that extend their digital control. These include:

- Blocking specific protocols for targeted websites;
- Shutting down internet access during political crises;
- Controlling software and algorithms using artificial intelligence techniques;
- Imposing strict content censorship; and
- Enforcing data localization laws that prohibit cross-border data transfers—as seen in jurisdictions such as Russia and China ²¹.

Conversely, states like the United States view cyberspace as a global commons (*res communis*) that should not be subjected to national sovereignty. Other nations adopt a different approach,

¹⁷ Ali Hassan Ali Bdour, Legal Protection to Keep Pace with Technology and Digital Transformation, *International Journal for Publishing Scientific Studies*, Vol. 15, No. 3, Tamim Center for Scientific Studies and Research, Hashemite Kingdom of Jordan, December 2022, p. 319.

¹⁸ The expression "digital public order" *ordre public numérique* has recently appeared in doctrinal literature to designate the fundamental values whose protection must be guaranteed by law in the digital society; see: Philippe Mouron & Cécile Piccio, *L'ordre public numérique*, PUAM, 2015.

¹⁹ Hassan Abou El-Kassim, The Concept of Digital Public Order, *Al-Bahith Journal for Legal and Judicial Studies and Research*, No. 57, Morocco, August 2023, p. 375.

²⁰ Pierre Bellanger, *Souveraineté numérique et ordre public Digital Sovereignty and Public Order*, *Archives de Philosophie du Droit*, Vol. 58, Dalloz, 2015, p. 285. Available at: <https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr><https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr>

²¹ Khadidja Ben Kelfat, The Repercussions of Cyber Warfare on Digital Sovereignty, *Journal of Algerian and Comparative Law*, Vol. 10, No. 2, University of Sidi Bel Abbès, December 2024, p. 288.

recognizing that cyberspace can pose a direct threat to their national security, thereby prompting them to enact stringent measures to control information flows and safeguard digital infrastructure ²².

However, alongside the immense benefits yielded by technology lies an equal degree of peril across multiple aspects of human life. Coupled with the borderless nature of the internet, a challenge no less critical emerges: cyberspace has transformed into a vast arena for various cyberattacks and cybercrimes. Consequently, legal intervention becomes an imperative necessity to counter these breaches by strengthening **cybersecurity**—which entails protecting systems, software, and networks from disruptive digital services that seek unauthorized access to sensitive information to alter, disable, or destroy it ²³.

In this context, public order must be understood not merely as a matter of physical security, but equally as one of **digital security**. This requires a smart integration of law and technology to effectively re-establish public order and curb illicit behaviors that compromise data and information security or endanger individual privacy and vital interests. This represents a central challenge for law enforcement authorities within an ever-evolving technological landscape ²⁴.

Cyberspace has impelled a fundamental re-examination of the concept of security—specifically regarding the threshold that enables states to shield themselves from emerging threats and protect critical infrastructure from the illicit use of information and communication technologies. The ²⁵ digital world has created a web of economic and social relations among diverse individuals across distinct social and cultural backgrounds. Consequently, several legal scholars have proposed adopting international legislation, delegating the framing of digital public order to international conventions and treaties that establish unified rules (*règles uniformes*).

Nevertheless, adopting international legislation may not resolve the issue without generating new challenges. Regulation by an international body is impractical to the extent that it cannot fully reflect individual national definitions of public order. What cyberspace truly requires is an **international social contract**—one that respects the diversity of national societies. In reality, anticipating an international agreement capable of accommodating all behaviors deemed harmful to domestic public order remains unlikely. As a result, the most viable path forward is the adaptation of national regulations protecting public order to the demands of cyberspace, supported by an international cooperation framework to suppress offenses against public order—a matter detailed below.

A-The Necessity of drafting a constitution specific for the Information Society

Legislative movements across the globe have attempted to frame the digital space through a corpus of virtual legal enactments. This new global digital environment has fostered a novel domain for behavioral regulation (*droit du comportement*), necessitating measures to combat hate speech, child exploitation and exposure to immoral content, incitement to violence, copyright infringements (piracy), fraud, money laundering, and malware attacks against electronic communications

²² Hadja Wafi, Digital Sovereignty and Cybersecurity in the Era of Artificial Intelligence: A Conceptual and Analytical Study of Challenges and Opportunities, in *The Uses of Artificial Intelligence in Enhancing Digital Sovereignty and Achieving Cybersecurity*, Layma Publishing, Kolea, Tipaza, Algeria, 2025, p. 15.

²³ Abdallah Boutaba & Toufik Bousti, The Role of Cybersecurity in Enhancing National Health Security, *Algerian Journal of Law and Political Science*, Vol. 9, No. 2, 2024, pp. 708–709.

²⁴ Cristian Cucoreanu, Public Order and the Technological Revolution: Implications for Police and Citizen Safety, *European Journal of Law and Public Administration*, Vol. 11, Issue 1, 2024, pp. 39–52. DOI: <https://doi.org/10.18662/eljpa/11.1/219> <https://doi.org/10.18662/eljpa/11.1/219>

²⁵ Amira Abdel-Azim Mohamed Abdel-Gawad, Cyber Risks and Means of Confronting Them in Public International Law, *Journal of Sharia and Law*, Vol. 35, Part 3, 2020, p. 377.

infrastructure—whether committed by individuals or by states for industrial or espionage purposes. In truth, significant legal loopholes remain to be addressed, compelling states to systematically review and update their legislative frameworks.²⁶

However, national legislative frameworks remain inherently insufficient to fully assert control over the digital space due to two main factors:

1-The Exponential Pace of Digital Advancement : Technological changes unfold at record speeds within a hyper-connected society, rendering complete control over this accelerated digital explosion virtually impossible.

2-The Manipulative Capacity of Digital Media : The limitless possibilities for content manipulation have led several legal scholars to assert the fundamental limitations of statutory law in governing cyberspace. Consequently, some argue for divesting states of exclusive regulatory authority, restricting regulation to technical domain solutions to avoid jurisdictional conflicts and working toward a **General Constitution for the Information Society** ²⁷.

In this context, numerous digital law scholars advocate for the adoption of international information legislation comprising technical standards and specifications inherent to the digital industry. These standards assert themselves as compelling rules (*normes de contrainte*) that cannot be ignored, fostering adherence to guiding principles and values aligned with fundamental human needs ²⁸. Furthermore, part of the legal doctrine emphasizes that national legislatures should resort ²⁹. to soft law instruments—such as digital codes of conduct or ethical charters—as non-binding frameworks. These instruments establish guiding principles and best practices to promote responsible internet usage among all stakeholders and address emerging issues, particularly within Artificial Intelligence (AI).

Nevertheless, formulating international legislation for cyberspace remains exceptionally difficult amid the ongoing restructuring of internet governance brought about by technological advancements. This shift has altered the overall distribution of power and the capacity to exercise fundamental rights and freedoms. System-level standards and protocols present distinct advantages and disadvantages regarding global oversight and control at a time of heightened technological polarization.

Moreover, the digital sphere gives rise to *de facto* authorities—private, non-state actors operating across national borders to provide essential public services to humanity. Transnational tech companies and internet service providers exercise immense technical power that may eclipse the capabilities of state governments themselves. The multiplicity of actors—encompassing not only sovereign states but also tech giants and digital media platforms possessing public power attributes—reflects a scenario where private entities exercise authority akin to state power. This dynamic demonstrates how technological drivers pose a fundamental challenge to the principle of the Rule of Law.

Accordingly, the crucial role played by telecommunication service providers and digital platforms in halting transmissions or removing unlawful content—which inflicts severe harm on individuals and society—must not be overlooked. Given that online platforms offer public-facing

²⁶ Ahmed Kharroubi, *Legislation Regulating the Digital Space in Algeria Between Technical Challenges and Future Infrastructure Stakes*, Journal of Library Science, Vol. 13, No. 1, Department of Library Science and Documentation, Faculty of Humanities, University of Algiers 2, 2021, p. 50.

²⁷ This is advocated by the International Telecommunication Union ITU; cited in Ismail Ougadi, *op. cit.*, p. 13.

²⁸ Ismail Ougadi, *op. cit.*, p. 13.

²⁹ Arnaud Sée, *La régulation des algorithmes: un nouveau mode de globalisation? Algorithm Regulation: A New Mode of Globalization?*, Revue de Droit Administratif, No. 5, 2019, pp. 830–836.

services and exercise authority analogous to administrative policing (police administrative), particularly regarding online information management they must be actively integrated into³⁰. content moderation. This can be achieved by imposing behavioral standards and regulatory compliance obligations aligned with local and international privacy and data protection regimes, thereby encouraging responsible conduct and preventing cyberspace from becoming a lawless realm (zone de non-droit).

A prime example is the European Union's **Digital Services Act (DSA)**, which obliges platforms to adopt a proactive approach to digital content moderation. The DSA mandates tech companies and online platforms to ensure a safe, transparent environment for users while safeguarding their rights under a unified regulatory scheme applied across EU Member States. Under this compliance framework, service providers face strict obligations—chiefly the swift removal of illegal content, child protection, and advertising transparency—backed by the authority to levy massive fines calculated as a percentage of the non-compliant entity's total annual global turnover.

While service providers may claim exemption from liability by acting promptly to prevent the dissemination of illegal content or material likely to breach public order, the disruption to public order does not cease upon content removal; it persists as long as the material remains accessible. Consequently, the European DSA aims to hold platforms accountable for removing illegal content before it achieves widespread dissemination, thereby safeguarding public order. Ultimately,³¹ holding private actors accountable is essential: public authorities alone cannot manage digital technology, and the rapid pace of technological change hastens the obsolescence of traditional regulatory frameworks. States are therefore increasingly turning to new approaches grounded in holding private entities—such as platforms and search engines—accountable, subjecting them to public order and moral standards, and deploying blocking measures (hachage / blocage) as a deterrent mechanism.

B- Algeria's Efforts to Establish and Preserve Digital Public Order

With the expansion of online activities within the digital space, there arose an urgent need for national legislation to keep pace with this transformation in order to safeguard digital rights and freedoms, ensuring they remain strictly within their governing legal framework. As law constitutes the expression of societal will, cyberspace has increasingly attracted all segments of Algerian society. This legislative adaptation to the digital era required the regulation of several economic activities in their electronic form, precipitating the enactment of **Law No. 18-05 on Electronic Commerce**³², which stands as a foundational text framing the digital economic public order.

Furthermore, the digital revolution mandated the transition of various traditional economic and professional activities into digital formats. This is notably reflected in **Law No. 04-08 relating to the Conditions for Exercising Commercial Activities**, as amended and supplemented which³³.

³⁰ Ahmed Saad Mohamed Hussein, Digital Constitutionalism Theory and the Protection of Constitutional Values and Rights in the Digital World, Journal of Legal and Economic Sciences, Vol. 67, No. 2, Faculty of Law Khartoum Branch, Cairo University, Egypt, July 2025, p. 2319.

³¹ Morgan Pénitot, Les modérateurs de plateformes en ligne : de nouveaux acteurs de police ? Online Platform Moderators: New Police Actors?, Cahiers de la recherche sur les droits fondamentaux, No. 21, Presses Universitaires de Caen, France, November 17, 2023, p. 45. DOI: <https://doi.org/10.4000/crdf.8824><https://doi.org/10.4000/crdf.8824>

³² Law No. 18-05 of 24 Sha'ban 1439 corresponding to May 10, 2018, relating to Electronic Commerce, Official Gazette of the People's Democratic Republic of Algeria, No. 28, published May 16, 2018.

³³ Law No. 04-08 of 27 Jumada II 1425 corresponding to August 14, 2004, relating to the Conditions for Exercising Commercial Activities, as amended and supplemented, Official Gazette of the People's Democratic Republic of Algeria, No. 52, published August 18, 2004.

prompted the issuance of **Executive Decree No. 18-112** establishing the model extract of the electronic commercial register -These developments compelled the legislature to harmonize pre³⁴. existing regulatory texts with current digital realities.

It is worth noting that the Law on Electronic Commerce was preceded by legislation governing the signature and authentication of electronic transactions through the enactment of **Law No. 15-04 of February 1, 2015, establishing the General Rules Relating to Electronic Signatures and Certification** through which the Algerian legislature sought to formulate a legal approach³⁵. operationalizing electronic evidence. Subsequently, the legislature repealed Law No. 15-04 by promulgating **Law No. 26-02 establishing the General Rules Relating to Trust Services for Electronic Transactions and Electronic Identification**, while maintaining its implementing decrees in force pending the issuance of new regulatory³⁶.

Law No. 26-02 represents one of the most critical recent digital laws in Algeria, establishing a unified, modern legal framework for trust in the digital environment. It resolves various concepts and procedures that were previously subject to regulatory fragmentation or doctrinal and practical debate under prior legislation, particularly the 2018 Law on Electronic Commerce.

The significance of Law No. 26-02 lies in its comprehensive scope: it extends beyond regulating electronic signatures to incorporate electronic seals, electronic time-stamps, registered electronic delivery services, website authentication certificates, electronic identification, electronic documents, and attribution (imputabilité). Moreover, it establishes a robust institutional framework anchored by the National Electronic Certification Authority, alongside a rigorous licensing and supervisory system for trust service providers. Consequently, Law No. 26-02 marks a qualitative leap in the legislative landscape, laying solid legal foundations for a secure digital economy, trustworthy electronic transactions, and effective legal protection for all parties.

In addition, **Law No. 18-07 relating to the Protection of Natural Persons in the Processing of Personal Data**³⁷ constitutes one of the most prominent statutes aimed at maintaining digital public order. It reinforced the existing legal framework with provisions designed to protect the economic, social, and psychological security of individuals by safeguarding their personal data and their right to privacy in the digital realm—an objective at the very core of digital public order.

To remedy the practical lacunae that emerged during the implementation of Law No. 18-07, it was amended by **Law No. 25-11 of August 5, 2025**. This amendment responded to the imperative of strengthening citizen protections against privacy infringements, aligning national legislation with international standards—most notably the European Union's General Data Protection Regulation (GDPR)³⁸—and resolving statutory gaps identified in the application of Law No. 18-07.

³⁴ Executive Decree No. 18-112 of 18 Rajab 1439 corresponding to April 5, 2018, establishing the Model Extract of the Commercial Register Issued Through Electronic Procedure, as amended and supplemented, Official Gazette of the People's Democratic Republic of Algeria, No. 21, published April 11, 2018.

³⁵ Law No. 15-04 of 11 Rabi' II 1436 corresponding to February 1, 2015, establishing the General Rules Relating to Electronic Signatures and Certification, Official Gazette of the People's Democratic Republic of Algeria, No. 06, published February 10, 2015.

³⁶ Law No. 26-02 of 29 Sha'ban 1447 corresponding to February 17, 2026, establishing the Rules Relating to Trust Services for Electronic Transactions and Electronic Identification, Official Gazette of the People's Democratic Republic of Algeria, No. 14, published February 18, 2026.

³⁷ Law No. 18-07 of June 1, 2018, relating to the Protection of Natural Persons in the Processing of Personal Data, Official Gazette of the People's Democratic Republic of Algeria, No. 34, published June 10, 2018.

³⁸ Regulation EU 2016/679 of the European Parliament and of the Council General Data Protection Regulation - GDPR of 2016, which entered into force on May 25, 2018, established core principles serving as a global reference framework for any collection or processing of personal data.

Among the most prominent amendments introduced by **Law No. 25-11** is the inclusion of new statutory definitions, such as biometric data and pseudonymization (pseudonymisation). Furthermore, the law established the position of Data Protection Officer (**DPO**) within every entity processing personal data. The DPO must be qualified to ensure regulatory compliance and serve as an interface or liaison with the National Authority for the Protection of Personal Data (**ANPDP**).

The legislation also expanded the powers of the ANPDP, strengthening its status as an independent administrative authority capable of conducting supervisory operations through regional hubs responsible for audit and oversight over data controllers and processors.³⁹ Under Article 43, the law mandates the maintenance of a dedicated register for data breaches. Additionally, Articles 41-bis(2) and 41-bis(3) require data controllers and sub-processors to maintain a record of processing activities in physical or electronic form, alongside an automated processing log to document all operations; these records must be placed at the disposal of the National Authority upon request. Moreover, the law reinforced the framework for cross-border data transfers by imposing strict conditions on transfers and onward transfers to third countries.

In practice, Law No. 25-11 represents a qualitative leap in personal data protection in Algeria, aligning national standards with international best practices and effective enforcement frameworks. The ultimate efficacy of this legislation remains contingent upon strengthening institutional capacity and enacting specific rules regulating Artificial Intelligence (AI).⁴⁰ Its practical success will depend heavily on the degree of compliance among economic actors, particularly enterprises. Consequently, raising awareness, delivering specialized training, and providing appropriate technical tools are essential to transforming this regulatory reform into a shared societal culture of data protection.

The true strategic challenge lies in building a sovereign digital ecosystem that places national interests at the core of technological advancement in a rapidly changing world. Today, sovereignty is no longer measured solely by geographic boundaries, but equally by who owns the data, controls payment gateways, and establishes the digital infrastructure upon which national economies operate. Just as cybersecurity is rooted in technology, it is equally anchored in trust—a trust cultivated when users feel that their data is protected, their digital rights are respected, and institutions remain transparent and responsive during cyberattacks or security breaches. This reality makes it imperative for corporations, institutions, and states to prioritize data security.

Accordingly, traditional goals of administrative policing (police administrative) have expanded to accommodate technological advances. In their modern form, these virtual administrative policing objectives manifest as **overarching cyber and information security**.⁴¹ Defined through its functional objectives, cybersecurity constitutes the body of activities that protects human and financial resources linked to information and communication technologies, minimizes damages and losses resulting from digital threats and breaches, and seeks to restore systems to their pre-incident status while remediating damage. It is further defined as the set of technical, organizational, and

³⁹ See: Article 27-bis of Law No. 25-11.

⁴⁰ Ahlam Boukhemis, The Problem of Enforcing Public Order on Social Media Among Content Creators, *Journal of Judicial Jurisprudence*, Vol. 16, No. 2, Laboratory of Judicial Precedent Impact on Legislative Movement, Mohamed Khider University of Biskra, October 2024, p. 194.

⁴¹ Souad Hassan & Zoubir Mekaoui, Protection of Personal Data in Light of Artificial Intelligence: A Reading of Algerian and International Legislation, *Conference Proceedings of the International Conference on Information Technology in the Era of AI and Digital Transformation* Cairo, Egypt, October 29–30, 2025, Democratic Arab Center for Strategic, Political, and Economic Studies, Berlin, Germany, 2025, p. 74.

administrative measures aimed at safeguarding information systems and networks from cyberattacks, ensuring the confidentiality, integrity, and availability (**CIA triad**) of data and information.

Consequently, modern public order within the digital space aims to adopt a comprehensive suite of tools, policies, security frameworks, and guidelines to mitigate and address information threats, leveraging best practices to protect the electronic environment and govern digital user assets.

In addition to the aforementioned legislation, several other legal texts aim directly or indirectly to establish or frame digital public order, highlighting the imperative of enhancing cybersecurity amid technological evolutions. Prioritizing information technology has become a cornerstone for advancing the national economy, necessitating robust cybersecurity to ensure data protection. Algeria has pursued this through a range of measures, beginning with the creation of the **Post and Electronic Communications Regulatory Authority (ARPCE)**—an independent legal entity established under Law No. 00-03 of August 5, 2000⁴². Following its repeal, it was replaced by **Law No. 18-04 of May 10, 2018, establishing the General Rules Relating to Post and Electronic Communications**⁴³, which renewed the authority's mandate to regulate the post and electronic communications market—a mechanism designed to prevent the misuse of information technology from infringing upon public rights, fundamental freedoms, and personal privacy in the digital environment.⁴⁴

It can be asserted that Algeria has achieved significant progress in developing the core infrastructure of the Information and Communication Technology (ICT) sector, with the initial contours of its transition toward digital transformation gradually taking shape. Furthermore, the state has moved to strengthen both the technical and regulatory dimensions of cybersecurity, concentrating these efforts primarily within the sphere of legal procedures.

This commitment is evidenced by **Law No. 09-04 of August 5, 2009, establishing Specific Rules for the Prevention and Control of Information and Communication Technology-Related Crimes**⁴⁵, which delineates under Article 4 the specific instances authorizing the interception and monitoring of electronic communications. Moreover, Article 13 mandated the creation of a national body dedicated to preventing and combating ICT-related offenses, which was subsequently operationalized following the issuance of **Presidential Decree No. 15-261 of October 8, 2015, establishing the Composition, Organization, and Functioning of the National Body for the Prevention and Control of Information and Communication Technology-Related Crimes**. Additionally, other specialized entities have been established to fulfill vital roles in countering various forms of cybercrime.⁴⁶

To meet these operational imperatives, **Presidential Decree No. 20-05 of January 20, 2020, establishing a National System for the Security of Information Systems** was promulgated⁴⁷. Article 3 structures this system around two key organs: the **National Council for the Security of**

⁴² Official Gazette of the People's Democratic Republic of Algeria, No. 48, published August 5, 2000.

⁴³ Official Gazette of the People's Democratic Republic of Algeria, No. 27, published May 13, 2018.

⁴⁴ Amine Belaroussi & Khaled Seriah, The Impact of Cybersecurity and Administrative Policing on Rights and Freedoms in the Digital Era, *Journal of Law, Society, and Power*, Vol. 14, No. 1, University of Oran 2 Mohamed Ben Ahmed, March 2025, p. 211.

⁴⁵ Official Gazette of the People's Democratic Republic of Algeria, No. 47, published August 16, 2009.

⁴⁶ Ikram Berkan & Fahim Ramli, The Reality and Problems of Cybersecurity in Algeria, Research Paper Presented at the 1st National Scientific Conference on Algeria's Grand Strategy for Achieving Comprehensive Security and Sustainable Development Goals, Faculty of Political Science, Saleh Boubnider University Constantine 3, February 2024.

⁴⁷ Presidential Decree No. 20-05 of 24 Jumada I 1441 corresponding to January 20, 2020, establishing a National System for the Security of Information Systems, Official Gazette of the People's Democratic Republic of Algeria, No. 04, published January 26, 2020.

Information Systems and the **National Agency for the Security of Information Systems**. This decree aims to protect digital data, combat cybercrime, and mitigate network intrusions by instituting an institutional and technical framework to secure national bodies.

As a novel legal framework strengthening cybersecurity and data protection within public institutions, **Presidential Decree No. 26-07** was issued⁴⁸, obligating all public institutions and administrative bodies to establish a specialized, technically autonomous internal unit charged with information system security. The responsibilities of this specialized structure encompass:

- **Formulating and implementing information security policies** and maintaining vigilance against cyber threats;
- **Protecting data** by ensuring the lawful processing of personal data;
- **Audit and oversight**, through conducting periodic security audits and promptly reporting information system security incidents; and
- **Structural organization**, by recruiting specialized personnel proficient in risk management, cyber threat intelligence, data protection, and awareness raising.

In recent years, the Algerian legislature has rectified—at least partially—the statutory void in the Penal Code regarding cybercrime. This was achieved through the enactment of **Law No. 04-15 of November 10, 2004, amending and supplementing the Penal Code**, which introduced Articles 394-bis through 394-bis(7) under a dedicated section titled "Offenses against Automated Data Processing Systems."

The offenses codified under these amendments include:

- **Unauthorized Access and Stay:** Penalized under Article 394-bis;
- **Data Alteration and Interference:** Penalized under Article 394-bis(1); and
- **Illicit Data Dealing:** Penalized under Article 394-bis(2).

Furthermore, Article 394-bis(3) doubles the prescribed penalties when the offense targets national defense or public law entities and institutions. Under Article 394-bis(4), the legislature imposed strict corporate criminal liability, subjecting legal persons that commit any of these offenses to fines equal to five times the maximum fine applicable to natural persons.

Additionally, Article 394-bis(5) provides that any individual participating in a group or agreement formed to prepare one or more of the aforementioned offenses shall face the same penalties prescribed for the completed offense. Article 394-bis(6) states that, without prejudice to the rights of bona fide third parties, courts shall order the confiscation of devices, software, and means utilized in the offense, along with the closure of the offending websites and the physical premises if the owner acted with knowledge. Finally, Article 394-bis(7) stipulates that attempting to commit any of these misdemeanors shall be punishable by the penalties prescribed for the completed offense.

Furthermore, in 2006, the Algerian legislature introduced new amendments targeting Section VII-bis of the Penal Code.⁴⁹ This amendment aimed to stiffen penalties for cybercrimes and infringements on individual privacy, particularly amid the proliferation of social media platforms.

⁴⁸ Presidential Decree No. 26-07 of 18 Rajab 1447 corresponding to January 7, 2026, establishing a Specialized Structure for Information Systems Security and Data Protection within Public Institutions, Administrations, and Bodies, and Determining Its Tasks, Organization, and Operation, Official Gazette of the People's Democratic Republic of Algeria, No. 04, 2026.

⁴⁹ See: Article 333-bis4 of Law No. 24-06 of 19 Shawwal 1445 corresponding to April 28, 2024, Official Gazette of the People's Democratic Republic of Algeria, No. 30, published April 30, 2024, amending and supplementing Order No. 66-156 of June 8, 1966, establishing the Penal Code.

Because cybercriminals are highly organized and adept, suppressing modern cybercrimes necessitates recalibrating both penal and procedural statutes while modernizing investigative methodologies that require cybersecurity monitoring. Consequently, justice enforcement authorities tracking cyber offenders must be digitally empowered and equipped with appropriate technical and legal tools—not only to better comprehend cybercrimes, but primarily to collect digital evidence effectively for prosecution, thereby upholding public order in the digital domain.

To this end, the Algerian legislature introduced under **Law No. 25-14 amending the Code of Criminal Procedure** a series of special investigative techniques tailored to the virtual realm, including the interception of communications, image capture, sound recording, and undercover operations (infiltration).⁵⁰

Additionally, expeditious procedures and communication mechanisms must be established to enable investigative authorities to liaise with foreign jurisdictions to gather evidence, within a framework of international judicial cooperation and mutual legal assistance—particularly regarding electronic evidence. Referring to **Law No. 09-04**, the Algerian legislature adopted a system of mutual legal assistance in alignment with international conventions—chiefly the **Budapest Convention on Cybercrime**, ratified by Algeria—and guided by the principle of reciprocity.

Recognizing that winning the cybersecurity challenge depends fundamentally on empowering human capital—from which skilled professionals capable of executing critical mandates emerge—**Presidential Decree No. 24-181** was enacted to establish the **National Higher School of Cybersecurity**.⁵¹ This institution is tasked with higher education, scientific research, and technological development in information systems security, delivering innovative, high-tech solutions to bolster national efforts.

At the highest executive level, Algeria has sought to transform public governance by laying the groundwork for a structured National Digital Strategy. The institutional architecture of digital transformation in Algeria centers on the **High Commissariat for Digitalization**, which is tasked with coordinating policies and implementing the **National Digitalization Strategy 2025–2030**. Nevertheless, despite these regulatory texts, the current legal framework remains fragmented and lacks comprehensiveness, highlighting the need for a unified, virtual legal framework to govern all aspects of digitalization.

It is worth noting that while the High Commissariat for Digitalization plays a vital role, it remains in its developmental phase and requires the support of specialized, independent supervisory bodies in domains such as personal data protection and cybersecurity. To ensure transparency and enforce digital rights, Algeria must evolve its institutional structure toward autonomous, specialized entities. In this regard, the Algerian legislature could draw inspiration from the Tunisian model, which established a dedicated Ministry of Communication Technologies directly overseeing digital affairs.⁵² Expanding the mandates of the High Commissariat to match a specialized ministry aligns with comparative models showing that independent, specialized bodies offer the most effective structure for achieving these strategic objectives.

⁵⁰ Law No. 25-14 of 9 Safar 1447 corresponding to August 3, 2025, amending and supplementing the Code of Criminal Procedure, Official Gazette of the People's Democratic Republic of Algeria, No. 54, published August 13, 2025.

⁵¹ Presidential Decree No. 24-181 of June 5, 2024, establishing the National Higher School of Cybersecurity, Official Gazette of the People's Democratic Republic of Algeria, No. 39, published June 8, 2024.

⁵² Kais Abna, The Virtual Legal Framework for Digital Transformation in Algerian Public Administration, Qabas Journal for Human and Social Studies, Vol. 9, No. 2, December 2025, p. 167.

Furthermore, increasing reliance on digital technology mandates a robust, secure infrastructure to preserve data privacy and mitigate cyber risks—particularly within Artificial Intelligence (AI) and cloud computing. The establishment of national data centers—such as the **Oran Data Center opened in 2025**—marks a pivotal milestone in enhancing Algeria’s digital infrastructure. Possessing a data center of this scale grants Algeria autonomy in data storage and processing, reduces dependence on foreign infrastructure, attracts global technology firms, fosters a fertile ecosystem for AI startups, and reinforces state capacity to protect data and monitor digital flows.

Finally, oversight and accountability mechanisms serve as essential pillars ensuring transparency and protecting digital rights. Restrictions on digital rights can only be justified based on objective criteria where competing public interests or third-party rights outweigh private interests. As judiciaries are compelled to balance digital rights and freedoms against broader public interests, an independent, impartial judiciary becomes paramount to ensure that any restriction adheres strictly to the principles of **proportionality and necessity**. This includes judicial review over administrative decisions—such as annulling arbitrary internet shutdowns or blocking electronic payment gateways—which directly impair digital socio-economic rights.⁵³

Conclusion

In light of the novel challenges posed by the digital space at a time when global competition to keep pace with rapid technological advancement is reaching its peak, there is an imperative need to secure a digital environment that is both safe and strictly compliant with the rule of law. Nevertheless, this legal field remains in a state of continuous evolution. With the expanding reliance on the internet and digital technologies, constantly updating and broadening electronic legislation has become indispensable to safeguarding user rights and preserving public order.

However, the primary challenge extends beyond merely enacting statutory texts; it lies in the state's capacity to operationalize these provisions and empower existing institutions to act as effective regulators of this domain—a goal that cannot be realized without robust enforcement mechanisms. Conversely, maintaining the delicate balance between protecting digital rights on the one hand and ensuring freedom of expression on the other will remain a rigorous test. Concerns that regulatory frameworks might serve as a pretext to restrict fundamental freedoms persist, necessitating clear constitutional and statutory safeguards.

Based on the findings of this study, the author proposes a series of measures aimed at framing the digital domain and reshaping the relationship between the state and its citizens in cyberspace, ensuring that regulation does not devolve into restriction, nor protection into paternalism:

- **Strengthening Enforcement and Multilateral Collaboration:** Legislation alone is insufficient unless reinforced by effective oversight mechanisms, close public-private partnerships, synergy between local expertise and international best practices, and active civil society engagement.
- **Formulating Clear Technology Governance Policies:** Law enforcement authorities must develop and implement comprehensive policies governing the operational use of technology, strictly ensuring the protection of citizens' constitutional rights.
- **Establishing Proactive Cybersecurity Protocols:** Robust digital infrastructure and specialized cybersecurity software must be deployed to provide proactive defense against digital risks, reduce the attack surface, and neutralize threats before they escalate into cyber incidents or disasters.

⁵³ Mohamed Sobhi Hassan Ali, Constitutional Protection of Digital Rights, op. cit., p. 429.

- **Investing in Advanced Cybersecurity and Real-Time Threat Detection:** Law enforcement agencies should invest heavily in technical solutions to safeguard sensitive data, prevent cyberattacks, and detect espionage or breach attempts in real-time, alongside mandatory information security training for personnel.

- **Establishing Sovereign National and Regional Data Centers:** Domestic data hosting infrastructure should be expanded to ensure that Algerian data is stored locally under rigorous security standards, thereby bolstering digital trust and fostering a data-driven economy.

- **Implementing Civic Education and Digital Rights Awareness Programs:** Targeted awareness programs should be rolled out to educate citizens on their digital rights, the lawful parameters of police technology usage, and mechanisms for enhancing cooperation with law enforcement.

- **Enhancing Applied Law Enforcement Training:** Training curricula for law enforcement officers must be modernized to incorporate practical instruction on emerging technologies—including simulations and case studies—to ensure rapid and effective incident response.

- **Promoting Academic and Policy Research:** Multidisciplinary research on the impact of technology on public order should be incentivized to identify best practices and formulate innovative solutions to contemporary digital challenges.

- **Providing Continuous Technical Training for Electronic Administrative Policing Authorities:** Regulators and enforcement personnel must undergo continuous professional development regarding modern technologies, software applications, and digital media to ensure greater efficacy in maintaining public order in the digital realm.

- **Empowering the Judiciary in the Digital Sphere:** Judicial authority must be reinforced to enable judges to strike a proportional balance between internet freedom, digital security imperatives, and constitutional guarantees. This requires specialized judicial training programs focused on analyzing digital rights and their technical complexities.

- **Harmonizing National Legislation with International Standards:** Domestic legal frameworks must be continuously adapted to align with global efforts aimed at establishing and preserving digital public order.

Bibliography

I. Legal Sources

A. National Legal Frameworks (Algeria)

- **Law No. 04-08** of 27 Jumada II 1425 corresponding to August 14, 2004, Relating to the Conditions for Exercising Commercial Activities, as amended and supplemented, Official Gazette of the People's Democratic Republic of Algeria, No. 52, published August 18, 2004.

- **Law No. 15-04** of 11 Rabi' II 1436 corresponding to February 1, 2015, Establishing the General Rules Relating to Electronic Signatures and Certification, Official Gazette of the People's Democratic Republic of Algeria, No. 06, published February 10, 2015.

- **Law No. 18-05** of 24 Sha'ban 1439 corresponding to May 10, 2018, Relating to Electronic Commerce, Official Gazette of the People's Democratic Republic of Algeria, No. 28, published May 16, 2018.

- **Law No. 18-07** of 17 Ramadan 1439 corresponding to June 1, 2018, Relating to the Protection of Natural Persons in the Processing of Personal Data, Official Gazette of the People's Democratic Republic of Algeria, No. 34, published June 10, 2018.

- **Presidential Decree No. 20-05** of 24 Jumada I 1441 corresponding to January 20, 2020, Establishing a National System for the Security of Information Systems, Official Gazette of the People's Democratic Republic of Algeria, No. 04, published January 26, 2020.

- **Law No. 24-06** of 19 Shawwal 1445 corresponding to April 28, 2024, Amending and Supplementing Order No. 66-156 of June 8, 1966, Establishing the Penal Code, Official Gazette of the People's Democratic Republic of Algeria, No. 30, published April 30, 2024.

- **Law No. 25-14** of 9 Safar 1447 corresponding to August 3, 2025, Amending and Supplementing the Code of Criminal Procedure, Official Gazette of the People's Democratic Republic of Algeria, No. 54, published August 13, 2025.

- **Law No. 26-02** of 29 Sha'ban 1447 corresponding to February 17, 2026, Establishing Rules Relating to Trust Services for Electronic Transactions and Electronic Identification, Official Gazette of the People's Democratic Republic of Algeria, No. 14, published February 18, 2026.

- **Presidential Decree No. 26-07** of 18 Rajab 1447 corresponding to January 7, 2026, Establishing a Structure Responsible for Information Systems Security and Data Protection in Public Institutions, Administrations, and Bodies, Official Gazette of the People's Democratic Republic of Algeria, No. 04, 2026.

- **Presidential Decree No. 24-181** of 28 Dhul-Qi'dah 1445 corresponding to June 5, 2024, Establishing the National Higher School of Cybersecurity, Official Gazette of the People's Democratic Republic of Algeria, No. 39, published June 8, 2024.

- **Executive Decree No. 18-112** of 18 Rajab 1439 corresponding to April 5, 2018, Establishing the Model Extract of the Commercial Register Issued Through Electronic Procedure, as amended and supplemented, Official Gazette of the People's Democratic Republic of Algeria, No. 21, published April 11, 2018.

B. Regional Legal Frameworks

- **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR), Official Journal of the European Union, L 119/1, May 4, 2016 (entered into force May 25, 2018).

II. References

A. Arabic References

1. General Treatises:

- Al-Sanhuri, Abdel-Razzak Ahmed. *Al-Waseet in the Explanation of the New Civil Law: Theory of Obligation in General – Sources of Obligation*. Halabi Legal Publications, Beirut, Lebanon, 2000.

2. Specialized Books:

- Al-Kilabi, Hussein Abdullah. *Contractual Public Order*. Al-Sanhuri Library, 1st ed., Beirut, Lebanon, 2016.

- Al-Bishri, Imad Tariq. *The Concept of Public Order in Theory and Practice: A Comparative Study Between Positive Law and Islamic Jurisprudence*. 1st ed., Al-Maktab Al-Islami, Beirut, Lebanon, 2005.

3. Articles, Conference Papers & Periodicals:

- Aina, Kais. "The Virtual Legal Framework for Digital Transformation in Algerian Public Administration." *Qabas Journal for Human and Social Studies*, Vol. 9, No. 2, El Oued University, Algeria, December 2025, pp. 155–170.

- Al-Allaq, Abdelkader. "The Problem of Defining the Concept of Public Order." *Al-Mi'yar Journal*, Vol. 10, No. 4, Tissemsilt University, December 2019, pp. 1–14.
- Al-Khatib, Mohammad Irfan. "Guarantees of Rights in the Digital Era: From Concept Evolution to Protection Shift – A Reading of European and French Legislation with Applications to Kuwaiti Law." *Kuwaiti Journal of Law, Special Supplement*, Vol. 42, No. 3, Part 1, Academic Publication Council, Faculty of Law, Kuwait University, May 2018 / Sha'ban 1439 AH, pp. 251–319.
- Amin, Ahmed Abdel-Hamid. "The Role of the Concept of Public Order in Protecting the Legality of Contracts and the Weaker Party." *Journal of the Faculty of Law*, Vol. 2, No. 1, Part 1, Minia University, Egypt, June 2019, pp. 70–202.
- Amira, Abdel-Azim Mohamed Abdel-Gawad. "Cyber Risks and Countermeasures in Public International Law." *Journal of Sharia and Law*, Vol. 35, Part 3, 2020, pp. 363–541.
- Badour, Ali Hassan Ali. "Legal Protection to Keep Pace with Technology and Digital Transformation." *International Journal for Publishing Scientific Studies*, Vol. 15, No. 3, Tamim Center for Scientific Studies and Research, Hashemite Kingdom of Jordan, December 2022, pp. 318–326.
- Belaroussi, Amine, and Khaled Seriah. "The Impact of Cybersecurity and Administrative Policing on Rights and Freedoms in the Digital Era." *Journal of Law, Society, and Power*, Vol. 14, No. 1, University of Oran 2 Mohamed Ben Ahmed, March 2025, pp. 198–216.
- Ben Kraïdem, Ghania. "Digital Rights: Reality and Challenges." *Journal of Comparative Legal Studies*, Vol. 7, No. 1, Hassiba Benbouali University of Chlef, 2020, pp. 2033–2051.
- Ben Khalfat, Khadidja. "Impacts of Cyber Warfare on Digital Sovereignty." *Journal of Algerian and Comparative Law*, Vol. 10, No. 2, Sidi Bel Abbès University, December 2024, pp. 280–299.
- Berkan, Ikram, and Fahim Ramli. "The Reality and Challenges of Cybersecurity in Algeria." Research Paper presented at the 1st National Scientific Conference on Algeria's Grand Strategy for Achieving Comprehensive Security and Sustainable Development Goals, Faculty of Political Science, Saleh Bounider University (Constantine 3), February 2024.
- Boukhemis, Ahlam. "The Problem of Enforcing Public Order on Social Media Among Content Creators." *Journal of Judicial Jurisprudence*, Vol. 16, No. 2, Laboratory of Judicial Precedent Impact on Legislative Movement, Mohamed Khider University of Biskra, October 2024, pp. 187–204.
- Boutabba, Abdellah, and Tewfik Bousti. "The Role of Cybersecurity in Enhancing National Health Security." *Algerian Journal of Law and Political Sciences*, Vol. 9, No. 2, 2024, pp. 706–731.
- Draï, Larbi. "The Dialectic of Balancing Digital Rights Exercise and Digital Sovereignty Protection in Algerian Legislation." *Human Rights and Public Freedoms Journal*, Vol. 11, No. 1, Faculty of Law and Political Science, Abdelhamid Ibn Badis University of Mostaganem, 2026, pp. 728–765.
- Hassan, Abou El-Kassim. "The Concept of Digital Public Order." *Al-Bahith Journal for Legal and Judicial Studies*, No. 57, Morocco, August 2023, pp. 365–380.
- Hassan, Souad, and Zoubir Mekaoui. "Protection of Personal Data under Artificial Intelligence: A Reading of Algerian and International Legislation." *Conference Proceedings of the International Conference on Information Technology in the Era of AI and Digital Transformation* (Cairo, Egypt, October 29–30, 2025), Democratic Arab Center for Strategic, Political, and Economic Studies, Berlin, Germany, 2025, pp. 64–77.

- Hussain, Ahmed Saad Mohamed. "Theory of Digital Constitutionality and the Protection of Constitutional Rights and Values in the Digital World." *Journal of Legal and Economic Sciences*, Vol. 67, No. 2, Faculty of Law (Khartoum Branch), Cairo University, Egypt, July 2025, pp. 2338–2474.
- Kharroubi, Ahmed. "Legislation Governing Digital Space in Algeria Between Technological Challenges and Future Infrastructure Stakes." *Journal of Library Science*, Vol. 13, No. 1, Department of Library Science and Documentation, University of Algiers 2, 2021, pp. 48–67.
- Milat, Abdelhafid. "The International Nature of the Internet and the Concept of Public Order: Determining Liability for Public Order Violations in Internet Hosting and Access Contracts." *Image and Communication Journal*, Vol. 5, No. 19, Laboratory of Mass Communication and Semiology of Visual Systems, University of Oran, 2016, pp. 29–38.
- Ougadi, Ismail. "Digital Space and the Need for a New Legal Paradigm." Takamoul Center for Studies and Research, January 15, 2021. Available at: [\(https://www.takamoul.org\]\(https://www.takamoul.org\)\) \(Accessed: May 12, 2026, 11:00 AM\).](https://www.takamoul.org](https://www.takamoul.org))
- Shafi, Majda Abdel. "Constitutional Protection of Cybersecurity and Its Impact on Public Order." *Journal of Legal and Economic Research*, Vol. 57, No. 4, Faculty of Law, Menoufia University, Egypt, pp. 345–410. Available at: [\(http://Jslem.journals.ekb.eg\]\(http://Jslem.journals.ekb.eg\)\) \(Accessed: December 1, 2024, 11:30 AM\).](http://Jslem.journals.ekb.eg](http://Jslem.journals.ekb.eg))
- Sobhi Hassan Ali, Mohamed. "Constitutional Protection of Digital Rights." *International Journal of Jurisprudence, Judiciary, and Legislation*, Vol. 6, No. 2, Egyptian Judges Club, 2025, pp. 412–439.
- Wafi, Hadja. "Digital Sovereignty and Cybersecurity in the Era of Artificial Intelligence: A Conceptual and Analytical Study of Challenges and Opportunities." In *The Uses of Artificial Intelligence in Enhancing Digital Sovereignty and Achieving Cybersecurity*, Laima Publishing, Kolea, Tipaza, Algeria, 2025, pp. 9–32.
- Abdo, Roqaya Saeed Abdel-Latif. "Risks of Modern Electronic Means on State Public Order." *The Legal Journal*, Vol. 22, No. 9, Faculty of Law (Khartoum Branch), Cairo University, Egypt, 2024, pp. 3449–3496.

B. French References

1. Books & Treatises:

- Lequette, Suzanne. *Droit du numérique*. LGDJ, Lextenso, France, 2024.
- Malaurie, Philippe. *La notion de l'ordre public et les bonnes mœurs en droit privé*. Rapport présenté dans le cadre des travaux de l'Association Henri Capitant pour la culture juridique française, t. 7, 1950.
- Mouron, Philippe, et Laurent Piccio. *L'ordre public numérique*. Presses Universitaires d'Aix-Marseille (PAUM), 2015.

2. Articles & Contributions:

- Bellanger, Pierre. « Souveraineté numérique et ordre public. » *Revue Archives de philosophie du droit*, Tome 58, Dalloz, 2015, pp. 285–302. Available at: [\(https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr\]\(https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr\)\)](https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr](https://droit.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285?lang=fr)).
- Penitot, Morgan. « Les modérateurs de plateformes en ligne : de nouveaux acteurs de police ? » *Cahiers de la recherche sur les droits fondamentaux*, n° 21, Presses universitaires de Caen, France, 17 novembre 2023, pp. 45–56. DOI: 10.4000/crdf.8824.

- Sée, Arnaud. « La régulation des algorithmes : un nouveau mode de globalisation ? » Revue de droit administratif, n° 5, 2019, pp. 830–836.

C. English References

- Cucoreanu, Cristian. "Public Order and the Technological Revolution: Implications for Police and Citizen Safety." European Journal of Law and Public Administration, Volume 11, Issue 1, 2024, pp. 39–52. DOI: 10.18662/eljpa/11.1/219.