

Dirassat & Abhath
The Arabic Journal of Human
and Social Sciences



مجلة دراسات وأبحاث
المجلة العربية في العلوم الإنسانية
والاجتماعية

EISSN: 2253-0363
ISSN : 1112-9751

Cybersecurity and Digital Privacy Protection in Algerian Legislation: A Comparative Analytical Study in Light of International Standards الأمن السيبراني وحماية الخصوصية الرقمية في التشريع الجزائري: دراسة تحليلية مقارنة في ضوء المعايير الدولية

Dr. Cheurfa Asma

¹ Associate Professor, Department of Media and Communication, Faculty of Humanities and Social Sciences, Badji Mokhtar University – Annaba, Algeria asma.cheurfa@univ-annaba.dz

د. شرفة أسماء

أستاذة محاضرة صنف أ ، قسم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة باجي مختار

عنابة، الجزائر، asma.cheurfa@univ-annaba.dz

تاريخ القبول : 2025/12/27

تاريخ الاستلام: 2025/09/23

Abstract :

This article addresses the issue of cybersecurity in the context of rapid digital transformations by examining national and international legal and regulatory frameworks related to data protection and digital privacy. Its main objective is to assess the adequacy of existing legislation in meeting current challenges, with a particular focus on the Algerian experience in light of comparative practices. The study is structured around three main axes: the conceptual framework of cybersecurity, international and national legal references, and the implications of such regulations for building digital trust. A descriptive-analytical approach was employed, based on a review of relevant legal and academic sources. The findings reveal that cybersecurity is no longer a purely technical matter but rather a strategic issue intersecting with legal and institutional dimensions. This calls for the development of comprehensive legislative frameworks and the reinforcement of digital governance mechanisms to protect cyberspace and foster trust among individuals and institutions.

Keywords : Cybersecurity; Data Protection; National and International Legislation; Digital Privacy; Digital Trust.

ملخص:

يهدف هذا المقال إلى إشكالية الأمن السيبراني في ظل التحولات الرقمية المتسارعة، من خلال البحث في الأطر القانونية والتنظيمية الوطنية والدولية المرتبطة بحماية البيانات والخصوصية الرقمية. يهدف إلى إبراز مدى كفاية التشريعات القائمة في مواجهة التحديات الراهنة، مع التركيز على التجربة الجزائرية في ضوء الممارسات المقارنة. تمت معالجة الموضوع عبر ثلاثة محاور أساسية: الإطار المفاهيمي للأمن السيبراني، المرجعيات القانونية الدولية والوطنية، ثم انعكاسات هذه التشريعات على بناء الثقة الرقمية. اعتمدت الدراسة منهجاً وصفيًا تحليليًا يقوم على مراجعة الأدبيات والمصادر القانونية والأكاديمية ذات الصلة. توصل المقال إلى أنّ الأمن السيبراني لم يعد قضية تقنية فقط، بل يمثل رهاناً استراتيجيًا يتقاطع مع أبعاد قانونية ومؤسسية. مما يفرض ضرورة تطوير الأطر التشريعية وتعزيز آليات الحوكمة الرقمية بما يضمن حماية الفضاء السيبراني وترسيخ الثقة لدى الأفراد والمؤسسات. الكلمات المفتاحية: الأمن السيبراني؛ حماية البيانات؛ التشريعات الوطنية والدولية؛ الخصوصية الرقمية؛ الثقة الرقمية.

1. INTRODUCTION

In today's digital society, the widespread integration of information and communication technologies into daily life has transformed not only the way individuals interact and exchange information but also the foundations of economic, political, and social structures. Online platforms, digital services, and electronic transactions have become indispensable, offering new opportunities for innovation and development. At the same time, however, these advancements have introduced unprecedented risks to personal data security and the protection of user privacy. Digital privacy is no longer a matter of individual choice; it has evolved into a collective concern and a fundamental human right that underpins personal dignity,

autonomy, and security¹. Ensuring this right requires not only technical safeguards but also comprehensive legal and institutional frameworks capable of addressing the complex challenges of cyberspace.

Within the Algerian context, the rapid adoption of digital technologies—ranging from e-commerce to e-governance and social networking—has heightened the urgency of establishing effective privacy protections. In response, Algerian lawmakers have introduced several legislative instruments, including Law No. 18-07 on the protection of natural persons in the processing of personal data and Law No. 18-05 regulating electronic commerce, in addition to constitutional guarantees that explicitly recognize the right to privacy and the confidentiality of communications². These efforts reflect Algeria's recognition of

the strategic importance of cybersecurity and the necessity of protecting citizens in the digital environment. Nevertheless, significant challenges persist. The dynamic nature of technological innovation often outpaces legislative development, leaving gaps in the scope and applicability of existing laws. Furthermore, limited institutional capacities to enforce these laws, coupled with users' lack of awareness about their digital rights, exacerbate vulnerabilities and undermine the effectiveness of legal protections³.

Given this reality, academic inquiry into the protection of user privacy in Algerian legislation is both timely and essential. This study adopts a descriptive and analytical approach that combines documentary research—examining constitutional provisions, legislative texts, and judicial interpretations—with comparative legal analysis, particularly referencing international standards such as the General Data Protection Regulation (GDPR). By situating Algerian legislation within the broader global discourse on data protection and digital rights, this research aims to assess the adequacy of existing measures, identify their limitations, and suggest avenues for improvement. Ultimately, the central research problem can be articulated as follows: *To what extent does Algerian legislation ensure the protection of user privacy in cyberspace, and what challenges hinder its effective implementation in comparison with international standards?*

2. Conceptual Framework

In order to provide a clearer understanding of the study, it is essential to establish a conceptual framework that defines the key concepts related to digital communication and online platforms. A well-structured conceptual framework not only clarifies the meanings of fundamental terms but also delineates the relationships among them, thus offering a coherent basis for the analysis. In the context of digital environments, concepts such as *user*, *user privacy*, *cybersecurity*, and *digital rights* are

central to both theoretical discussions and practical implications. Each of these concepts represents a cornerstone in analyzing how individuals interact with digital platforms, how their personal data is managed, and how their rights are preserved in cyberspace. Therefore, this section is devoted to providing detailed definitions and explanations of these key terms, setting the stage for a more comprehensive understanding of the research problem.

A) User:

The term user refers to any natural or legal person who utilizes information and communication technologies, whether directly through computers, smartphones, or indirectly via digital platforms and online services. This concept encompasses individual citizens, private organizations, and public institutions engaged in digital interactions. In the legal context, the user is considered the most vulnerable actor in cyberspace, as they are exposed to risks such as privacy violations, data theft, and unlawful exploitation of personal information⁴. Consequently, users occupy a central position in legislative frameworks that aim to regulate digital transactions and provide legal safeguards against cybercrimes⁵.

B) User Privacy:

User privacy denotes an individual's right to control their personal data and determine how it is collected, processed, stored, and shared by third parties. It is recognized as a fundamental right closely linked to human dignity, identity protection, and personal security⁶. The importance of user privacy has grown significantly with the expansion of digital services, which require vast amounts of sensitive information such as financial, medical, or biometric data⁷. In Algerian legislation, this right is protected by constitutional provisions and reinforced by specific laws, notably *Law No. 18-07 on the protection of natural persons in the processing of personal data*. This law⁸ establishes legal standards for handling personal data and prescribes sanctions for

violations. As such, user privacy serves as a cornerstone for building trust in the digital environment and strengthening cybersecurity measures.

C) Cybersecurity:

Cybersecurity encompasses the set of policies, technologies, and practices designed to protect information systems, networks, and data from cyber threats and malicious attacks⁹. It involves preventing hacking, safeguarding critical infrastructures, ensuring the confidentiality and integrity of data, and mitigating risks of breaches or leaks¹⁰. From a legal perspective, cybersecurity extends beyond technical protection to include legislative and regulatory dimensions, where laws are enacted to govern digital behaviors and assign responsibilities¹¹. In Algeria, increasing attention is devoted to cybersecurity through national strategies against cybercrime and legal measures that criminalize activities endangering information security¹². Thus, cybersecurity represents the overarching framework that ensures safe, secure, and responsible use of digital spaces.

D) Digital Rights:

Digital rights are the extension of fundamental human rights into the digital realm. They include the right to privacy, freedom of expression, access to information, digital security, and the protection of personal data¹³. These rights are essential for enabling individuals to fully benefit from digital transformation without compromising their freedoms or exposing themselves to undue risks¹⁴. At the international level, digital rights have gained prominence, particularly through frameworks such as the European Union's *General Data Protection Regulation (GDPR)*¹⁵, which sets high standards for user protection in cyberspace. In Algeria, elements of digital rights are recognized in constitutional provisions and specific laws governing media and e-commerce¹⁶. However, the main challenge lies in their effective enforcement and in achieving a balance between national cybersecurity

requirements and respect for users' digital freedoms.

3. Cybersecurity

Cybersecurity has evolved from a predominantly technical field into a multidisciplinary domain that encompasses policy, law, organizational management, and social behaviour. The scholarly literature can be grouped into several interrelated strands: historical evolution and conceptual framing; technical and organizational measures; governance and legal approaches; the human and social dimension; capacity building and resilience; and international cooperation and transnational challenges. Each strand sheds light on the complexity of securing digital environments and offers lessons relevant to national strategies.

A) Historical evolution and conceptual framing

Early work framed cybersecurity as an extension of information security — focused on confidentiality, integrity and availability (the CIA triad) — and concentrated on protecting IT assets from unauthorized access and disruption¹⁷. Over time, two developments broadened the field: the expansion of cyberspace into socio-technical systems (including IoT, cloud services, and critical infrastructures) and the recognition of cyber operations as instruments of statecraft and national security¹⁸. Contemporary conceptual treatments therefore emphasize cybersecurity as both a technical discipline and a strategic policy domain that intersects with economic stability, public safety, and human rights¹⁹.

B) Technical and organizational measures

A large body of literature evaluates technical controls (firewalls, intrusion detection systems, encryption, secure software development) and organizational practices (incident response teams, security policies, risk assessments) as core defenses²⁰. Research highlights the importance of adopting a “defence-in-depth” posture where multiple layers of controls mitigate diverse attack vectors²¹. Recent studies further stress emerging technical challenges: securing cloud architectures, managing the attack

surface of IoT devices, and addressing vulnerabilities introduced by machine learning systems. Security-by-design and privacy-by-design principles are repeatedly advocated to integrate protection early into systems life cycles²².

C) Governance and legal approaches

Scholars examine how national laws, regulatory frameworks, and institutional arrangements shape cybersecurity outcomes. Comparative analyses contrast centralized, state-led models with pluralistic, multi-stakeholder approaches that involve private sector actors and civil society²³. Policy literature underscores the need for clear legal definitions (cybercrime, digital evidence), proportionate powers for investigation, and oversight mechanisms that maintain rights protections while enabling effective enforcement²⁴. The interplay between data protection regimes (e.g., GDPR) and cybersecurity regulation is also a major focus, with authors arguing for regulatory coherence to avoid gaps and contradictions²⁵.

D) Human and social dimensions

A persistent finding across studies is that the human factor remains the weakest link: social engineering, phishing, poor password hygiene, and insider threats account for a significant share of successful breaches²⁶. Research in behavioural cybersecurity recommends combining technical solutions with education, awareness campaigns, and incentive structures to promote safer practices among users and employees²⁷. Organizational culture—leadership commitment, cross-functional collaboration, and continuous training—emerges as a decisive variable in resilience²⁸.

E) Capacity building and resilience

The literature highlights the importance of investing in national capabilities: skilled workforce development, digital forensics, national CERTs/CSIRTs, and public sector modernization²⁹. Measurement studies (e.g., national cybersecurity indices) reveal disparities across countries in legal frameworks, technical readiness, and

cooperation capacity. Scholars recommend a whole-of-society approach that balances immediate operational needs (incident detection, response) with long-term investments (research, higher education, industry partnerships) to build lasting resilience³⁰.

F) International cooperation and transnational challenges

Cyber threats routinely cross borders, creating jurisdictional, evidentiary, and diplomatic complications. Academic analyses emphasize the limits of unilateral approaches and the utility of multilateral instruments (mutual legal assistance, information-sharing frameworks) as well as voluntary public-private partnerships for real-time threat intelligence³¹. At the same time, tensions persist around sovereignty, data localization, and divergent legal standards. Authors call for pragmatic, incremental cooperation—focused on shared priorities like critical infrastructure protection and child online safety—while continuing dialogue on norms for state behaviour in cyberspace³².

J) Synthesis and implications for national strategies

The literature converges on several themes relevant to national cybersecurity planning: (1) cybersecurity must be framed as a socio-technical challenge requiring coordinated policy, legal, technical and social interventions; (2) prevention and resilience depend equally on technology, governance, and human capacity; (3) alignment between data protection and security rules reduces regulatory friction; and (4) international and regional cooperation is essential to contend with transnational threats³³. For countries developing their frameworks, the evidence suggests prioritizing capacity building (CERTs, forensics, skilled personnel), establishing clear legal authorities with human-rights safeguards, and institutionalizing public-private collaboration for information sharing and incident response.

H) Relevance to Algeria (brief linkage)

Applying these lessons, Algeria's cybersecurity development could usefully emphasize: strengthening national incident response capabilities and digital forensics; integrating security-by-design requirements into public procurements and e-government projects; expanding professional training and university curricula in cyber disciplines; and pursuing regional cooperation arrangements to expedite cross-border investigations. Ensuring legal clarity and harmonization between data protection law and cybercrime statutes will help avoid enforcement gaps while protecting citizens' digital rights.

4. Legal Framework in Algeria

Algeria has developed a comprehensive legal framework to address the challenges of cybersecurity, user protection, and digital rights in the context of increasing digitalization. This framework combines constitutional provisions, specific legislation, and regulatory measures to ensure the protection of individuals and institutions in cyberspace. The following key instruments form the backbone of Algeria's legal response to cybersecurity and user privacy.

A) Law on the Prevention and Fight Against Cybercrime

The Law on the Prevention and Fight Against Cybercrime, initially enacted in 2009 and subsequently amended to adapt to evolving threats, establishes the legal basis for criminalizing activities that endanger digital security. It defines a broad range of offenses, including unauthorized access to information systems, data manipulation, identity theft, and dissemination of malicious software³⁴. The law also provides mechanisms for investigation, prosecution, and international cooperation in combating cybercrime, reflecting Algeria's recognition of the transnational nature of digital threats³⁵. Importantly, the legislation assigns specific responsibilities to internet service providers (ISPs) and digital operators, requiring them to collaborate with law

enforcement agencies when cybercrimes are detected³⁶.

B) Law No. 18-05 on E-Commerce

Law No. 18-05, enacted in 2018, regulates electronic transactions and seeks to foster trust in online commercial activities. It establishes the legal validity of electronic contracts, digital signatures, and electronic payments³⁷. The law also imposes obligations on e-commerce operators to protect consumer rights, ensure transparency, and safeguard personal data. A critical dimension of this law is its intersection with cybersecurity, as it prescribes standards for secure online transactions and imposes penalties for fraudulent practices in digital markets³⁸. By doing so, Law 18-05 aims to promote economic development through digital trade while ensuring user confidence in online platforms.

C) Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Law No. 18-07 represents a cornerstone in Algeria's approach to safeguarding user privacy. Adopted in 2018, it aligns with international standards such as the European Union's General Data Protection Regulation (GDPR) by granting individuals the right to control how their personal data is collected, stored, and shared³⁹. The law creates an independent authority responsible for supervising compliance, authorizing data processing activities, and sanctioning violations⁴⁰. It also introduces principles such as data minimization, purpose limitation, and informed consent, thereby strengthening legal safeguards against misuse of personal information⁴¹. This legislation has been critical in establishing a culture of accountability among public and private entities handling sensitive user data.

D) Constitutional Guarantees Related to Privacy and Communication

The Algerian Constitution enshrines fundamental rights that extend into the digital domain. Provisions guarantee the right to privacy, the confidentiality of communications, and the protection of personal correspondence⁴². These constitutional rights provide the overarching legal basis for subsequent legislation on cybersecurity, data protection, and e-commerce. They also reflect Algeria's commitment to upholding human dignity and personal freedoms in the digital age. However, balancing these rights with national security concerns—particularly in the fight against cybercrime—remains a challenge⁴³.

Together, these legislative instruments form an integrated framework designed to secure cyberspace, protect users, and promote trust in digital platforms. Nonetheless, the effectiveness of this framework depends not only on the existence of laws but also on their enforcement, public awareness, and the capacity of institutions to adapt to the rapidly evolving digital landscape.

IV : Mechanisms of Privacy Protection

The effectiveness of privacy protection in Algeria depends not only on the existence of legal frameworks but also on the mechanisms that ensure their practical implementation. These mechanisms cover data protection during processing by both public and private entities, the liability of Internet Service Providers (ISPs) and digital platforms, and the supervisory role of the National Authority for the Protection of Personal Data. Together, they form an integrated system aimed at safeguarding user privacy and enhancing trust in cyberspace.

A) Data Protection During Processing by Public and Private Entities

Law No. 18-07 on the protection of natural persons in the processing of personal data establishes clear obligations for public institutions and private companies that collect or process user data⁴⁴. These entities

must ensure lawful, fair, and transparent processing of personal information, in line with principles such as purpose limitation, data minimization, and security safeguards⁴⁵. For instance, sensitive categories of data—such as medical or biometric information—require heightened levels of protection and cannot be processed without explicit consent⁴⁶. Furthermore, organizations are required to adopt technical and organizational measures to prevent unauthorized access, data leaks, or breaches, which aligns Algerian law with international standards like the GDPR⁴⁷.

B) Liability of ISPs and Digital Platforms

Internet Service Providers (ISPs) and online platforms play a central role in privacy protection due to their position as intermediaries between users and digital services. Under Algerian cybercrime and e-commerce legislation, ISPs are legally obliged to cooperate with authorities in cases of cybercrime investigations and to preserve digital evidence when required⁴⁸. At the same time, they bear responsibility for implementing technical safeguards to protect users' data from unauthorized access or exploitation⁴⁹. Digital platforms, especially those engaged in e-commerce and social networking, are expected to comply with transparency obligations, provide clear terms of service, and inform users about how their data is processed⁵⁰. Liability mechanisms thus serve as deterrents against negligence and encourage platforms to adopt privacy-by-design strategies.

C) The Role of the National Authority for the Protection of Personal Data

A cornerstone of Algeria's privacy protection system is the creation of the National Authority for the Protection of Personal Data, established by Law No. 18-07⁵¹. This independent body is entrusted with supervising the implementation of data protection standards, authorizing data processing operations, and ensuring

compliance by both public and private entities⁵². It also has the power to investigate violations, impose administrative sanctions, and raise awareness about digital rights among citizens⁵³. In addition, the authority acts as a mediator between users and organizations, handling complaints and ensuring that individuals' rights to access, rectify, or delete their personal data are effectively enforced⁵⁴. By exercising these supervisory functions, the authority contributes to building a culture of accountability and strengthens trust in digital ecosystems.

Taken together, these mechanisms represent a multidimensional approach to privacy protection. They establish responsibilities across different stakeholders—state institutions, private companies, ISPs, and digital platforms—while empowering an independent supervisory authority to enforce compliance. This institutional and legal synergy is crucial for ensuring that privacy rights in Algeria are not merely theoretical guarantees but practical realities in the age of digital transformation.

5. Challenges and Limitations

While Algeria has taken important steps toward strengthening its cybercrime framework, significant challenges remain that hinder the full effectiveness of these efforts. These challenges are both structural and contextual: they relate to the level of digital literacy among users, the technical capacities of institutions tasked with detection and enforcement, the adaptability of legislation to fast-changing technologies, and the complexity of managing cybercrimes that transcend national borders. Addressing these limitations is crucial, as they not only slow down institutional responses but also leave individuals, organizations, and the broader digital ecosystem vulnerable to evolving threats.

A) Lack of digital awareness among users

Despite rapid growth in connectivity—33.49 million internet users in January 2024 (≈72.9% penetration)—many users still lack practical cyber-hygiene skills (e.g., safe

authentication, privacy settings, reporting harms).⁵⁵ Recent field research on Algerian university students documents mixed or low cybersecurity awareness and uneven readiness to respond to online harms, indicating gaps between basic knowledge and secure day-to-day practices⁵⁶. In response, authorities and sectoral partners have launched awareness drives (e.g., 2025 campaigns targeting parents, educators and children), which underscores both policy attention and the persistence of the underlying problem⁵⁷. Region-wide threat assessments likewise urge sustained user-level education as a first line of defense.

B) Limited technical capacities for monitoring and investigation of cybercrimes

Capacity indicators highlight structural constraints in technical, organizational, and cooperative readiness. Algeria's ITU Global Cybersecurity Index profile (most recently published for 2020) recorded modest scores across legal, technical, organizational, capacity-building, and cooperation pillars, signaling room for improvement in incident detection, digital forensics, and coordinated response⁵⁸. Comparative indices also place Algeria in the lower middle tier of national readiness (e.g., NCSI position and sub-scores)⁵⁹. While a national incident response function exists—DZ-CERT, hosted at CERIST, acting as a focal point for threat information and coordination—its public footprint and published operational guidance remain comparatively lean⁶⁰. Specialized bodies created by Law 09-04 (e.g., the national organ for prevention and the fight against ICT-related offences) provide an institutional anchor, but reports emphasize the continuing need for tooling, training, and inter-agency workflows to keep pace with evolving threats⁶¹.

C) Gaps in legislation compared with fast technological change

Like many jurisdictions, Algeria faces a moving target: cloud, AI, IoT, biometrics, end-to-end encryption, and platformized data flows evolve faster than statutory updates and secondary regulations. Policy

analysis stresses that new technologies often require new or adapted regulatory approaches (risk-tiering, co-regulation, agile guidelines, and interoperability with international standards)⁶². This creates frictions in practice—e.g., uncertainty about lawful bases for emerging data uses, sector-specific security baselines, algorithmic accountability, and cross-border data transfers—until implementing rules, supervisory guidance, and technical standards mature. In the interim, institutions must translate high-level mandates into operational controls and audit mechanisms, an iterative process that can lag innovation cycles⁶³.

D) Difficulties in addressing cross-border cybercrimes

UNODC's global studies show that 30–70% of cybercrime incidents have a transnational element, making timely access to evidence across jurisdictions a frequent bottleneck⁶⁴. Even with model tools and practical guides for electronic evidence, formal mutual legal assistance (MLA) processes can be slow relative to the volatility of digital data.⁶⁵ Additionally, Algeria is not a Party to the Council of Europe's Budapest Convention on Cybercrime (checked against the official Parties list), which limits streamlined cooperation channels available under that instrument; cooperation therefore relies on bilateral arrangements, general MLA treaties, Arab League instruments, or ad-hoc mechanisms.⁶⁶ Relatedly, as of the African Union's official list (12 May 2023), Algeria had not signed or ratified the Malabo Convention on Cybersecurity and Personal Data Protection, attenuating regional harmonization leverage for cross-border requests and shared standards.⁶⁷ Together, these factors complicate rapid evidence preservation, authentication, and admissibility when perpetrators, victims, service providers, and servers span multiple countries.⁶⁸

6. International Experiences in User Privacy and Cybersecurity

The study of international experiences in the protection of user privacy and cybersecurity provides a comparative lens through which Algeria can strengthen its own legal and institutional framework. While the Algerian model has made important strides, it remains at an early stage of development compared to global benchmarks. By examining the European, American, Asian, and Arab approaches, Algeria can identify both challenges and opportunities that could guide its policies toward building a safer and more reliable digital ecosystem.

A) The European Experience

The European Union (EU) has become the global leader in digital rights protection, primarily through the implementation of the General Data Protection Regulation (GDPR), which entered into force in 2018⁶⁹. The GDPR represents a comprehensive and unified framework that applies to all EU member states, ensuring that the collection, processing, and storage of personal data are subject to strict conditions. One of its most significant features is the principle of informed consent, requiring organizations to clearly inform users about the use of their data and to obtain explicit permission before processing it. Another cornerstone is the "right to be forgotten", which grants individuals the legal power to request the deletion of their personal information from databases when it is no longer relevant⁷⁰.

In addition, the GDPR establishes severe financial penalties for organizations that fail to comply with data protection rules, thereby ensuring accountability and deterrence. Importantly, it also introduces the concept of Data Protection Officers (DPOs) in organizations handling sensitive data, ensuring continuous monitoring and compliance⁷¹.

For Algeria, the European experience offers valuable lessons, particularly in strengthening institutional oversight and creating independent bodies capable of enforcing laws effectively. Furthermore, Algeria could draw inspiration from the GDPR's emphasis on user empowerment and public awareness campaigns, which are

essential for building trust in digital services.

B) The American Experience

The United States follows a more sectoral approach to data protection, where different industries are governed by specific laws. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates the protection of health-related information, while the Children's Online Privacy Protection Act (COPPA) governs the collection of personal data from children under 13 years old⁷². Unlike the EU's centralized model, the U.S. approach is characterized by a decentralized framework, where state-level regulations (such as the California Consumer Privacy Act, CCPA) coexist with federal laws.

Another hallmark of the American system is the reliance on public-private partnerships. Major technology companies, such as Google, Microsoft, and Meta, invest heavily in cybersecurity infrastructure and collaborate with governmental agencies like the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA)⁷³. These partnerships facilitate real-time information sharing, early detection of cyber threats, and the development of innovative technological solutions.

For Algeria, the American model underlines the importance of involving the private sector as an active partner in cybersecurity. Instead of limiting responsibility to state institutions, Algeria could benefit from encouraging cooperation with Internet Service Providers (ISPs), financial institutions, and private tech companies. This would foster a multi-stakeholder approach, increasing resilience against cyber threats and enhancing the efficiency of monitoring systems.

C) The Asian Experience

Asia provides a diverse set of models that combine technological innovation with strict governance mechanisms. For instance, South Korea has developed one of the most advanced national cybersecurity strategies, relying on constant cyber drills and

proactive investment in research and development⁷⁴. Similarly, Japan has established a legal and institutional framework that prioritizes data security, coupled with international cooperation in cyber defense through organizations such as the OECD and the G7⁷⁵.

By contrast, China adopts a highly centralized approach, where the government exercises strong control over digital infrastructures through the Cybersecurity Law of 2017. This law requires companies to store personal data within the country and grants the state broad powers to monitor and regulate online activities⁷⁶. While this model has raised debates regarding human rights and freedom of expression, it has proven effective in limiting cybercrime and ensuring state control over critical infrastructures.

For Algeria, the Asian experiences highlight the importance of capacity building through technological investment and professional training. Algeria could also benefit from proactive strategies, such as periodic cyber drills and simulation exercises, which would prepare institutions to respond rapidly to cyberattacks. Furthermore, the emphasis placed by Asian countries on integrating cybersecurity into broader national strategies could inspire Algeria to adopt a more holistic, forward-looking approach.

D) The Arab Experience

The Arab world has made notable progress in recent years by aligning national legislation with international standards. The United Arab Emirates (UAE) introduced a federal law on data protection in 2021, establishing clear rules for data processing, cross-border data transfer, and user consent⁷⁷. Similarly, Saudi Arabia has set up the National Cybersecurity Authority, which coordinates national strategies, issues regulations, and oversees institutional compliance across government and private sectors⁷⁸.

In addition, Arab states have promoted regional cooperation, particularly through the Arab League Convention on Combating Information Technology Offences (2010),

which seeks to harmonize legal definitions and criminalize cyber offenses across member states⁷⁹.

For Algeria, the Arab experience is particularly relevant because of the cultural and legal similarities. It highlights the benefits of institutional coordination and the creation of specialized national authorities with strong enforcement powers. Furthermore, Algeria could strengthen its role within regional cooperation frameworks, allowing for joint initiatives, information sharing, and cross-border mechanisms to combat cybercrime more effectively.

7. Future Challenges to Cybersecurity and User Privacy and the Legal Measures Required

The digital landscape is constantly evolving, and with it, the nature of cybersecurity threats and the risks to user privacy are becoming increasingly complex. While Algeria has made progress in adopting legal frameworks to address existing issues, several future-oriented challenges demand urgent attention to ensure that legislation remains adaptive and effective. These challenges encompass technological, social, and legal dimensions.

A) Emerging Technological Threats

The rapid growth of new technologies such as artificial intelligence (AI), the Internet of Things (IoT), and cloud computing is expected to create vulnerabilities that cybercriminals can exploit⁸⁰. For example, AI can be used to conduct sophisticated cyberattacks such as deepfakes or automated phishing campaigns, while IoT devices often lack robust security standards, making them easy targets. These developments pose risks not only to individual users but also to national infrastructures. To address these threats, Algeria must adopt forward-looking regulations that integrate cybersecurity requirements into the design of emerging technologies.

B) Datafication and Big Data Risks

The exponential growth of big data analytics means that enormous amounts of personal information are collected, stored, and

processed daily⁸¹. While this data can drive innovation in sectors like healthcare, finance, and governance, it also increases the risk of mass surveillance, data misuse, and breaches. Future Algerian legislation should therefore impose stricter conditions on data minimization, transparency, and accountability, ensuring that data collection serves legitimate purposes without infringing on user rights.

C) Cross-Border Cybercrimes and Jurisdictional Dilemmas

As digital interactions are inherently global, future cybercrimes will increasingly involve cross-border dimensions⁸². Hackers may operate from outside Algeria, targeting national institutions, businesses, or citizens, making it difficult to investigate and prosecute offenders. Current legal frameworks often struggle with jurisdictional conflicts and the lack of effective international cooperation. Algeria will need to strengthen bilateral and multilateral agreements, harmonize its laws with international conventions, and participate actively in regional and global cybersecurity initiatives.

D) Digital Awareness and Social Engineering

Despite technological advances, the human factor remains one of the weakest links in cybersecurity. Techniques such as social engineering, phishing, and identity theft exploit users' lack of awareness⁸³. In the future, as digital services expand further into daily life, the risk of manipulation will rise. Legal measures should be complemented by national awareness campaigns, digital literacy programs, and institutional initiatives to train users in recognizing and avoiding cyber risks.

E) Balancing Security with Digital Rights

A key challenge for the future will be balancing national security needs with the protection of individual digital rights. Overly restrictive regulations risk undermining freedom of expression, access

to information, and privacy guarantees⁸⁴. Conversely, weak regulations expose users and institutions to cyber threats. For Algeria, the legal response must be a balanced one—introducing robust cybersecurity measures while embedding safeguards that protect constitutional rights and align with international human rights standards.

8. Conclusion

The analysis of Algeria's digital legal framework and mechanisms of privacy protection highlights both significant progress and persistent gaps. Algeria has enacted important legislation, including the Law on the Prevention and Fight against Cybercrime (2009), the E-commerce Law No. 18-05 (2018), and the Data Protection Law No. 18-07 (2018). Together with constitutional guarantees on privacy and communication, these laws form the cornerstone of the national approach to safeguarding user rights in cyberspace⁸⁵. Yet, rapid technological change, the global nature of cyber threats, and the evolving practices of malicious actors demand continuous adaptation and reinforcement of both law and practice⁸⁶. Against this backdrop, several key recommendations emerge.

A) Strengthening the legislative framework through international alignment

Algeria's cyber legislation, while comprehensive in scope, requires further harmonization with international standards such as the Budapest Convention on Cybercrime and the EU's General Data Protection Regulation (GDPR)⁸⁷. Alignment would not only improve the effectiveness of legal tools for investigation and prosecution but also facilitate cross-border cooperation, a crucial factor given the transnational nature of cybercrime⁸⁸. Moreover, embedding "privacy by design" and "security by design" principles in national regulations would ensure that future digital services integrate protection mechanisms from their inception⁸⁹.

B) Supporting the role of the judiciary in digital privacy cases

Laws alone are insufficient without effective judicial interpretation and enforcement. Scholars emphasize that judicial bodies play a decisive role in shaping how digital rights are applied in practice⁹⁰. For Algeria, this implies strengthening judicial training in cyber law, digital forensics, and international cooperation mechanisms⁹¹. Specialized judicial chambers or cybercrime courts could provide faster, more consistent rulings and contribute to jurisprudential clarity in cases involving personal data breaches, unauthorized surveillance, or online identity theft⁹².

C) Promoting user and institutional awareness

The literature consistently identifies the "human factor" as the weakest link in cybersecurity⁹³. In Algeria, limited awareness among end-users and organizations increases vulnerability to phishing, malware, and data misuse⁹⁴. To address this, large-scale awareness campaigns, integration of cybersecurity modules into school and university curricula, and targeted training for employees in sensitive sectors (finance, healthcare, government) are recommended⁹⁵. Public institutions, in particular, should be equipped with clear guidelines on data handling and accountability to ensure that citizens' digital rights are effectively protected.

D) Enhancing international cooperation against transnational cybercrime

Cyber threats disregard national borders, making unilateral approaches insufficient. International best practices stress the importance of bilateral and multilateral agreements for intelligence sharing, evidence exchange, and capacity building⁹⁶. Algeria could benefit from deeper engagement with African Union strategies, Mediterranean regional initiatives, and United Nations programs on cybercrime. Such cooperation would enable the country to access advanced expertise, benefit from

early-warning systems, and contribute to collective resilience in the face of global threats.

In conclusion, Algeria stands at a critical juncture: it has laid the legal foundations for digital privacy protection, but sustained efforts are required to ensure that these frameworks remain effective and future-proof. Legislative alignment, judicial empowerment, societal awareness, and international cooperation constitute the four pillars of a robust cybersecurity and privacy strategy. By consolidating these areas, Algeria can both protect its citizens' digital rights and position itself as a regional leader in cyber governance.

¹ Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2021.

² Algerian Official Gazette, Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, 2018. Algerian Official Gazette, Law No. 18-05 Regulating Electronic Commerce, 2018, Constitution of Algeria, Article 46: The right to privacy and confidentiality of communications, 2020.

³ Nir Kshetri, "Cybersecurity in Developing Nations: Challenges and Policy Options," *Computer*, Vol. 52, No. 6, 2019, pp. 64–68. <https://doi.org/10.1109/MC.2019.2909760>

⁴ Jan van Dijk, *The Network Society*, Sage Publications, 2020.

⁵ Manuel Castells, *The Rise of the Network Society*, Wiley-Blackwell, 2011.

⁶ Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2021.

⁷ Herman T. Tavani, *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*, Wiley, 2016.

⁸ République Algérienne Démocratique et Populaire, Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes

physiques dans le traitement des données à caractère personnel, *Journal Officiel*, 2018.

⁹ David Craigen, Nadia Diakun-Thibault & R. Purse, "Defining Cybersecurity," *Technology Innovation Management Review*, Vol. 4, No. 10, 2014, pp. 13–21.

¹⁰ P.W. Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.

¹¹ Nir Kshetri, *Cybersecurity and Cybercrime in Developing Countries*, Springer, 2019.

¹² Centre National de la Sécurité des Systèmes d'Information (CNSSI), *Stratégie nationale de cybersécurité en Algérie*, Alger, 2020.

¹³ Rebecca MacKinnon, Elonnai Hickok, Allon Bar & H. Lim, *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO, 2014.

¹⁴ Engin Isin & Evelyn Ruppert, *Being Digital Citizens*, Rowman & Littlefield, 2015.

¹⁵ European Union, *General Data Protection Regulation (GDPR)*, *Official Journal of the European Union*, 2016.

¹⁶ République Algérienne Démocratique et Populaire, *Constitution of Algeria (as amended)*, 2018.

¹⁷ Rossouw von Solms & Johan van Niekerk, "From information security to cyber security," *Computers & Security*, Vol. 38, 2013, pp. 97–102.

¹⁸ Joseph S. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, 2010

¹⁹ David Craigen, Nadia Diakun-Thibault, and Roberth Purse, "Defining cybersecurity," *Technology Innovation Management Review*, Vol. 4, No. 10, 2014, p. 13–21.

²⁰ Peter Warren Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.

²¹ ISO/IEC, *ISO/IEC 27001: Information Security Management Systems*, 2013.

- ²² Nir Kshetri, "Cybersecurity in Developing Nations: Challenges and Policy Options," *Computer*, Vol. 52, No. 6, 2019, pp. 64–68. <https://doi.org/10.1109/MC.2019.2909760>
- ²³ Laura DeNardis, *The Global War for Internet Governance*, Yale University Press, 2014.
- ²⁴ R. Broadhurst, "Developing Transnational Cybercrime Cooperation," *Journal of International Commercial Law and Technology*, Vol. 1, No. 1, 2006, pp. 19–34.
- ²⁵ Paul De Hert & Vagelis Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" *Computer Law & Security Review*, Vol. 32, No. 2, 2016, pp. 179–194.
- ²⁶ Kevin Mitnick & William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, 2011.
- ²⁷ Kathryn Parsons et al., "The human factor: Re-examining the role of users in cyber security," *Computers & Security*, Vol. 45, 2014, pp. 36–48.
- ²⁸ Sounil S., "Organizational culture and cybersecurity: bridging the gap," *Journal of Cyber Policy*, Vol. 5, No. 2, 2020, pp. 240–256.
- ²⁹ ENISA, *Threat Landscape Reports*, 2018.
- ³⁰ ITU, *Global Cybersecurity Index 2020*, 2020.
- ³¹ UNODC, *Comprehensive Study on Cybercrime*, 2013.
- ³² Martha Finnemore & Duncan Hollis, "Norms and cyber operations: state practice and evolving international law," *International Studies Quarterly*, Vol. 60, No. 3, 2016, pp. 472–484.
- ³³ OECD, *Enhancing the Governance of Cybersecurity*, OECD Publishing, 2019.
- ³⁴ République Algérienne Démocratique et Populaire, *Law No. 09-04 on the Prevention and Fight Against Cybercrime*, *Journal Officiel*, 2009.
- ³⁵ Nir Kshetri, *Cybersecurity and Cybercrime in Developing Countries*, Springer, 2019.
- ³⁶ INTERPOL, *African Cybercrime Legislation: A Comparative Review*, Lyon, 2021.
- ³⁷ République Algérienne Démocratique et Populaire, *Law No. 18-05 on E-Commerce*, *Journal Officiel*, 2018.
- ³⁸ OECD, *E-commerce in the Time of COVID-19*, Paris: OECD Publishing, 2020.
- ³⁹ République Algérienne Démocratique et Populaire, *Law No. 18-07 on E-Commerce*, *Journal Officiel*, 2018.
- ⁴⁰ European Data Protection Board (EDPB), *Guidelines on Data Protection Authorities*, Brussels, 2018.
- ⁴¹ Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.
- ⁴² République Algérienne Démocratique et Populaire. (2020). *Constitution of Algeria (as amended)*. *Journal Officiel*.
- ⁴³ MacKinnon, R., Hickok, E., Bar, A., & Lim, H. (2014). *Fostering Freedom Online: The Role of Internet Intermediaries*. UNESCO.
- ⁴⁴ République Algérienne Démocratique et Populaire. (2018). *Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data*. *Journal Officiel*.
- ⁴⁵ Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2021.
- ⁴⁶ Herman T. Tavani, *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*, Wiley, 2016.
- ⁴⁷ DataReportal, *Digital 2024: Algeria*, Global Digital Insights, 23 Feb 2024.
- ⁴⁸ République Algérienne Démocratique et Populaire, *Law No. 09-04 on the Prevention and Fight Against Cybercrime*. *Journal Officiel*, 2009.
- ⁴⁹ INTERPOL, *African Cybercrime Legislation: A Comparative Review*, Lyon: INTERPOL, 2021.
- ⁵⁰ République Algérienne Démocratique et Populaire, *Law No. 18-05 on E-Commerce*, *Journal Officiel*, 2018.
- ⁵¹ République Algérienne Démocratique et Populaire, *Law No. 18-07 on the Protection*

of Natural Persons in the Processing of Personal Data, Journal Officiel, 2018.

⁵² European Data Protection Board (EDPB), *Guidelines on Data Protection Authorities*, Brussels, 2018.

⁵³ Nir Kshetri, *Cybersecurity and Cybercrime in Developing Countries*, Springer, 2019.

⁵⁴ Rebecca MacKinnon, Elonnai Hickok, Allon Bar, and Hyeon Lim, *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO, 2014.

⁵⁵ DataReportal. "Digital 2024: Algeria." 23 Feb 2024. [DataReportal – Global Digital Insights](#)

⁵⁶ Abdelkader Brada and Fella Dahmani, "The Level of Cybersecurity Awareness and Cybercrime Response among Internet Users in Algeria," *El-Ryssala for Media Studies*, Vol. 8, No. 3, November 2024, ASJP.

⁵⁷ SAMENA Council. "Algeria launches nationwide awareness campaign to promote child online safety." 10 Feb 2025. [samenacouncil.org](#)

⁵⁸ INTERPOL. African Cyberthreat Assessment 2024. 2024. [Interpol](#)

⁵⁹ ITU. Global Cybersecurity Index 2020 – Algeria Country Profile. 2020.

⁶⁰ National Cyber Security Index (NCSI). "Algeria – 2022 profile." [ncsi.ega.ee](#)

⁶¹ CERIST. "DZ-CERT: Algerian Computer Emergency Response Team." [cerist.dz](#)

⁶² Council of Europe – Octopus Community. "Algeria (institutions and Law No. 09-04 summary)." [Portal](#)

⁶³ OECD. "Why New Technologies Need New Regulations." 1 Mar 2023.

⁶⁴ African Union / DataProtection.Africa. "List of countries which have signed/ratified the AU Convention on Cybersecurity and Personal Data Protection (Malabo)." List dated 12 May 2023. [dataprotection.africa](#)

⁶⁵ Council of Europe. "Budapest Convention on Cybercrime – List of Parties." Accessed Sept 2025.

⁶⁶ UNODC. Comprehensive Study on Cybercrime (2013) – findings on the transnational dimension of cybercrime. [Office des Nations Unies contre la drogue](#)

⁶⁷ UNODC. Practical Guide for Requesting Electronic Evidence Across Borders (2019; updates referenced 2022). [Office des Nations Unies contre la drogue+1](#)

⁶⁸ Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

⁶⁹ Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2020.

⁷⁰ Cécile Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law & Security Review*, Vol. 34, No. 1, 2018, p. 134–153.

⁷¹ Paul M. Schwartz and Daniel J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *New York University Law Review*, Vol. 86, 2011, p. 1814.

⁷² Joseph S. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, 2010.

⁷³ Sangbae Lee, "South Korea's Cybersecurity Strategy," *East Asia Forum*, 2014.

⁷⁴ Takashi Hara, "Japan's National Cybersecurity Strategy," *Journal of Cyber Policy*, Vol. 3, No. 1, 2018, p. 24–40.

⁷⁵ Rogier Creemers, *China's Cybersecurity Law: An Introduction*, Leiden Asia Centre, 2017.

⁷⁶ United Arab Emirates, *Federal Decree-Law No. 45 on the Protection of Personal Data*, 2021.

⁷⁷ National Cybersecurity Authority (Saudi Arabia), *National Cybersecurity Strategy*, 2020.

⁷⁸ League of Arab States, *Arab Convention on Combating Information Technology Offences*, 2010.

⁷⁹ Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum

Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crotoft, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodei, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *arXiv preprint*, arXiv:1802.07228, 2018.

⁸⁰ Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, 2013.

⁸¹ Ronald Broadhurst, "Developing Transnational Cybercrime Cooperation," *Journal of International Commercial Law and Technology*, Vol. 1, No. 1, 2006, p. 19–34.

⁸² Kevin Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, 2011.

⁸³ Paul De Hert and Vagelis Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" *Computer Law & Security Review*, Vol. 32, No. 2, 2016, p. 179–194.

⁸⁴ Karim Benyekhlef, "Digital Rights in the Maghreb: Developments and Challenges," *Journal of Cyber Policy*, Vol. 4, No. 3, 2019, pp. 255–272.

⁸⁵ Joseph Samuel Nye, *Cyber Power*, Belfer Center for Science and International Affairs, 2010.

⁸⁶ Council of Europe, *Budapest Convention on Cybercrime*, Strasbourg, 2001.

⁸⁷ Ronald Broadhurst, "Developing Transnational Cybercrime Cooperation," *Journal of International Commercial Law and Technology*, Vol. 1, No. 1, 2006, pp. 19–34.

⁸⁸ Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2011.

⁸⁹ Florence Bignami, "Comparative Law and the Right to Privacy in Europe and the

United States," *Yale Journal of International Law*, Vol. 43, No. 2, 2018, pp. 241–286.

⁹⁰ United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime*, United Nations, 2013.

⁹¹ Eneken Tikk, Mika Kerttunen, "The Role of National Courts in Cyber Law," *Journal of Law & Cyber Warfare*, Vol. 7, No. 1, 2018, pp. 45–67.

⁹² Kevin Mitnick, William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2011.

⁹³ Kathryn Parsons, Andrew McCormac, Marcus Butavicius, Malcolm Pattinson, Cate Jerram, "The Human Factor: Re-examining the Role of Users in Cyber Security," *Computers & Security*, Vol. 45, 2014, pp. 36–48.

⁹⁴ International Telecommunication Union (ITU), *Global Cybersecurity Index 2020*, ITU, 2020.

⁹⁵ Organisation for Economic Co-operation and Development (OECD), *Enhancing the Governance of Cybersecurity*, OECD Publishing, 2019.

⁹⁶ African Union, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)*, 2014.