Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

Article history (leave this part):
Submission date: 26.12-2024
Acceptance date: 24-05-2026
Available online: 10-06-2026
Keywords:
Right, Digital Privacy, Violation, Digital Surveillance, Personal Data Protection, Algerian Law, GDPR, Human Rights
Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Competing interest:
The author(s) have declared that no **competing interests**exist.
Cite as (leave this part):
Hanan Abufares Elkhimry;. (2024).Title.Journal of Science and Knowledge Horizons: 4(1), 283-293. https://doi.org/10.34118/jskp.v2i02.2727

The authors (2026). This Open Access article is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License (CC BY-NC 4.0) (http://creativecommons.org/licenses/by-nc/4.0/). Non-commercial reuse, distribution, and reproduction are permitted with proper citation

Journal of Science and Knowledge Horizons
ISSN 2800-1273-EISSN 2830-8379

Digitalization and the Human Right to Privacy: An Algerian Legal Perspective in Light of International Standards

Dr. Fahima BELHAMZI*
[1] Abdelhamid Ibn Badis University of Mostaganem (Algeria), fahima.belhamzi@univ-mosta.dz
https://orcid.org/0009-0009-1833-4889

Abstract:

This article examines the implications of digitalization for the human right to privacy, with a particular focus on the Algerian legal framework governing the protection of personal data. It addresses the transition from classical privacy to digital privacy, where personal information is continuously collected, stored, analysed and reused by public and private actors. The study asks whether existing legal instruments, especially Algerian Law No. 18-07, provide sufficient protection against contemporary risks such as digital surveillance, unauthorized processing, platform-based profiling and cross-border data exploitation. Using a descriptive, analytical and comparative legal approach, the article combines doctrinal analysis with a focused comparison between Algerian law and the European Union General Data Protection Regulation (GDPR). It also draws on the Cambridge Analytica case to demonstrate how apparently consensual data collection can become a large-scale violation of informational privacy. The findings show that Algerian legislation has established important guarantees, including consent, information, access, rectification, objection, regulatory control and sanctions. However, the effectiveness of this protection remains limited by weak practical enforcement, insufficient public awareness, the absence of a fully operational culture of compliance, and the need for clearer rules on algorithmic profiling, data portability, breach notification and international transfers. The article recommends strengthening the National Authority, developing sector-specific compliance guidelines, improving digital literacy, aligning selected mechanisms with GDPR standards and ensuring that digital transformation remains compatible with human dignity and fundamental rights.

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

Introduction

Digitalization has transformed privacy from a relatively stable legal and social concept into a dynamic and vulnerable condition. In the classical understanding, privacy was mainly associated with the home, correspondence, family life and personal reputation. In the digital environment, however, private life is increasingly translated into data traces: identifiers, messages, browsing behaviour, geolocation, biometric information, health data, social-media interactions and financial transactions. These traces may be processed at a speed and scale that traditional legal categories were not designed to anticipate.

The right to privacy remains a fundamental human right recognized in international instruments, constitutional provisions and ordinary legislation. Yet digitalization changes the form of the threat. Violations are no longer limited to physical intrusion or the publication of private information; they now include automated profiling, opaque data collection, unauthorized reuse of information, surveillance infrastructures, commercial exploitation and the permanent storage of personal data. For this reason, the protection of digital privacy has become one of the central legal and ethical questions of contemporary human rights law.

In Algeria, the constitutional recognition of private life and the adoption of Law No. 18-07 on the protection of natural persons in the field of processing personal character data represent significant legal progress. Nevertheless, the effectiveness of this protection must be assessed in light of the specific risks created by digital platforms, the expansion of public and private databases, cross-border data transfers and the limited awareness of data subjects regarding their rights. This reveals a research gap: Algerian law provides a formal framework for data protection, but its practical capacity to respond to complex digital harms remains insufficiently analysed in comparison with international standards such as the GDPR.

Accordingly, the central research question is: To what extent have Algerian and international legal frameworks succeeded in providing adequate protection for the right to digital privacy in the age of digitalization? This question leads to three sub-questions: What is the legal meaning of digital privacy? What risks do modern technologies create for the right to privacy? And how can Algerian law be strengthened through comparison with international models?

The article adopts a descriptive, analytical and comparative methodology. The descriptive approach is used to clarify the legal meaning of privacy and personal data. The analytical approach examines Algerian constitutional and legislative provisions, particularly Law No. 18-07. The comparative approach highlights selected points of convergence and divergence between Algerian law and the GDPR. The article also integrates a practical case study, the Cambridge Analytica scandal, to connect legal analysis with real-world risks.

Literature Review

Existing literature on privacy generally agrees that digitalization has expanded the scope of private life beyond physical spaces. Zein Al-Abidin (2016) emphasizes the international and

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

national dimensions of personal data protection, while Baji (2020) presents privacy as a concept whose legal meaning evolves with technological and social transformations. Hamidani (2019) focuses on breaches of privacy in the digital world and argues that technological progress requires renewed legal safeguards.

Several Algerian studies examine Law No. 18-07 as a response to the risks of personal data processing. Al-Eidani (2018) and Hezam (2019) underline the rights granted to data subjects and the obligations imposed on data processors. Their analyses confirm the importance of consent, access, rectification and objection, but they remain mainly descriptive. They do not sufficiently evaluate whether these mechanisms are effective when applied to algorithmic profiling, large-scale surveillance, artificial intelligence systems or cross-border platforms.

International literature has increasingly linked privacy to democratic accountability, platform governance and informational power. The Cambridge Analytica case demonstrated that users may formally share data within digital platforms while remaining unaware of its later political and commercial exploitation (Schneble et al., 2018; Hinds et al., 2020). Comparative scholarship on data protection also shows that the GDPR has become an influential model because it combines substantive rights, procedural duties, regulatory independence and strong sanctions. This article contributes to the existing literature by linking Algerian law to these international developments and by moving the analysis from a purely descriptive presentation of legal texts toward an assessment of their adequacy.

THE FIRST TOPIC: THE CONCEPTUAL AND LEGAL FOUNDATIONS OF THE RIGHT TO DIGITAL PRIVACY

First Section: Definition and Characteristics of the Right to Privacy

First Branch: Definition of the Right to Privacy

The right to privacy is one of the rights attached to human personality. It protects the individual's private sphere, dignity, correspondence, personal identity and control over personal information. Its importance lies in enabling individuals to decide what aspects of their lives may be disclosed and what aspects must remain protected from intrusion. In this sense, privacy is not merely secrecy; it is also the legal power to control access to one's personal life.

Internationally, Article 12 of the Universal Declaration of Human Rights prohibits arbitrary interference with privacy, family, home or correspondence, and protects individuals against attacks on honour and reputation. The same principle appears in the International Covenant on Civil and Political Rights. Nationally, the Algerian Constitution of 2020 guarantees the protection of private life and the secrecy of correspondence, while ordinary legislation enables individuals to seek protection against unlawful infringement of personality rights.

Digital privacy is the contemporary extension of this right. It concerns the protection of personal information in digital environments, including data collected through websites, applications, social networks, electronic transactions, connected devices and public databases. It also

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

includes the right of individuals to be informed about the processing of their data and to object to uses that violate their legitimate interests. Law No. 18-07 is therefore not separate from the right to privacy; it operationalizes this right in relation to personal data processing.

Second Branch: Characteristics of the Right to Privacy

The right to privacy has several characteristics. First, it is a personality right, attached to the individual by virtue of being human. Second, it is non-pecuniary in principle, even though violations may produce material and moral damage. Third, it is relative and variable, because its meaning depends on social, cultural, religious and technological contexts. Fourth, it is not absolute: it may be restricted by law for legitimate reasons such as public order, criminal investigation or national security, but such restrictions must remain necessary, proportionate and subject to judicial or independent oversight.

The digital environment intensifies this relativity. Individuals voluntarily disclose personal information on platforms, but this does not mean that they renounce privacy. Consent given in a complex digital interface may be formal rather than informed. Therefore, modern privacy protection must go beyond the idea that users are fully responsible for everything they share online. It must also regulate the institutions that collect, analyse and monetize personal data.

Second Section: The Impact of Modern Technologies on the Right to Privacy

First Branch: Risks of Modern Technologies to the Right to Privacy

Modern technologies create multiple risks for digital privacy. The first risk is mass collection. Public bodies and private companies can gather large quantities of data from administrative records, online accounts, payment systems, mobile phones and connected objects. The second risk is secondary use, where data collected for one purpose is later reused for another purpose without meaningful consent. The third risk is profiling, through which algorithms infer preferences, political opinions, economic status, health conditions or behavioural patterns. The fourth risk is data breach, where weak security exposes personal information to unauthorized access.

Digital surveillance also raises serious human rights concerns. Surveillance cameras, geolocation systems, biometric databases and platform monitoring may be justified by security or administrative efficiency, yet they may also normalize permanent observation. The danger is not only that data may be stolen, but also that individuals may adapt their behaviour because they feel constantly monitored. Thus, privacy is linked to freedom of expression, freedom of movement and democratic participation.

Commercial platforms present an additional challenge. Their economic model often depends on attention, prediction and targeted advertising. Users are encouraged to disclose information, while platforms transform this information into behavioural profiles. This creates an asymmetry of knowledge and power: the platform knows a great deal about the individual, whereas the individual often does not know how their data is used, shared or monetized.

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

Second Branch: Practical Illustration - The Cambridge Analytica Case

The Cambridge Analytica scandal provides a clear example of the vulnerability of digital privacy. Data from millions of Facebook users was collected through a third-party application and later used for political profiling and targeted messaging. The importance of the case lies in the fact that the violation did not occur through a traditional intrusion into private homes or correspondence. It occurred through platform-based data extraction, consent ambiguity and secondary use of personal information.

This case demonstrates three lessons relevant to Algerian and international law. First, privacy violations may be collective: the misuse of one person's data can also expose the data of their contacts. Second, consent is insufficient when users do not understand the consequences of data sharing. Third, regulatory authorities need investigative powers and deterrent sanctions capable of addressing powerful digital actors. The case therefore supports the argument that legal protection must combine individual rights with institutional accountability.

THE SECOND TOPIC: LEGAL PROTECTION OF PERSONAL DATA IN ALGERIAN LAW

First Section: Principles of Personal Data Protection under Law No. 18-07

First Branch: Consent, Lawfulness and Data Quality

Law No. 18-07 establishes a legal framework for the protection of natural persons in the field of personal data processing. It requires that personal data be processed lawfully and fairly, collected for specified, explicit and legitimate purposes, and kept accurate, complete and up to date. It also requires that data not be retained in a form allowing identification for longer than necessary. These principles reflect the movement from abstract privacy protection to concrete obligations imposed on data controllers and processors.

Consent occupies a central place in this framework. Article 7 requires the prior consent of the data subject for the processing of personal data and recognizes the possibility of withdrawal. However, consent is not always required where processing is necessary to comply with a legal obligation, protect the vital interests of the person, perform a contract or implement legally authorized measures. This structure is important, but it requires strict interpretation to prevent exceptions from becoming a general justification for excessive processing.

Data quality is also essential. If data is inaccurate, excessive or retained beyond its purpose, the risk to privacy increases. In the digital environment, inaccurate data can produce automated decisions that affect access to services, employment, credit, insurance or public administration. Therefore, the principle of data quality must be understood as a guarantee of fairness, not merely as an administrative requirement.

Second Branch: Rights of the Data Subject

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

Law No. 18-07 grants several rights to the person concerned by data processing. The right to information requires the processor to inform the individual clearly about the identity of the controller, the purpose of processing, recipients of the data, consequences of processing, available rights and possible international transfers. This right is crucial because individuals cannot exercise control over data processing if they do not know that processing is taking place.

The right of access enables individuals to know whether their data is processed, the purposes of processing, the categories of data involved, the recipients and the source of the data. The right to rectification allows the individual to request correction, updating, deletion or restriction of data processed contrary to legal requirements. The right to object protects the individual against processing that affects legitimate interests, particularly in relation to promotional or commercial purposes. Together, these rights form the procedural core of digital privacy protection.

Second Section: Obligations, Supervision and Sanctions

First Branch: Obligations of the Data Processor

The data processor must implement technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, damage, unauthorized disclosure or unauthorized access. These obligations require more than formal legal compliance. They imply risk assessment, cybersecurity measures, staff training, internal documentation and careful selection of external processors. External processors must act according to the instructions of the controller and must provide sufficient guarantees of security and confidentiality.

The confidentiality obligation is particularly important. Persons who have access to personal data because of their professional functions must preserve confidentiality even after the end of their duties. This rule recognizes that privacy violations may occur not only through cyberattacks, but also through internal misuse, negligence or unauthorized disclosure by individuals within institutions.

Second Branch: National Authority and Sanctions

Law No. 18-07 provides for the intervention of the National Authority responsible for the protection of personal data. The Authority receives declarations, grants authorizations where processing presents risks, monitors compliance and may impose administrative measures. The law also provides for criminal sanctions in serious cases, including unlawful processing, processing without required consent or authorization, false declarations, continuation of processing after withdrawal of authorization and fraudulent collection of personal data.

These mechanisms are necessary, but their effectiveness depends on institutional capacity. A legal text cannot protect privacy unless the supervisory authority has independence, technical expertise, sufficient resources, clear procedures and the ability to cooperate with other national

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

and international regulators. Therefore, the future of Algerian digital privacy protection depends not only on the existence of Law No. 18-07 but also on its practical implementation.

THE THIRD TOPIC: COMPARATIVE PERSPECTIVE AND EVALUATION OF LEGAL ADEQUACY

First Section: Comparison between Algerian Law and the GDPR

A comparison with the GDPR helps identify the strengths and limits of the Algerian framework. Both Algerian Law No. 18-07 and the GDPR recognize principles of lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation and security. Both frameworks also grant rights to individuals, including information, access, rectification and objection. This indicates that Algerian law is aligned with several core principles of modern data protection.

However, the GDPR provides more detailed mechanisms in several areas. It explicitly regulates data portability, automated decision-making, data protection by design and by default, data protection impact assessments, breach notification and the role of data protection officers. It also establishes a strong sanctioning model and a developed culture of compliance. Algerian law contains important guarantees, but it would benefit from clearer operational rules in these areas, especially as public services, banking, health, education and digital platforms increasingly rely on data-intensive systems.

The comparison does not mean that Algeria should mechanically copy the GDPR. Legal transplantation must consider national institutions, administrative capacities and socio-economic realities. Nevertheless, selected GDPR mechanisms can provide useful guidance for improving Algerian practice, especially regarding accountability, transparency, breach notification, privacy by design and independent supervision.

Second Section: Evaluation of the Adequacy of Protection

The Algerian legal framework has made real progress by recognizing personal data protection as a legal necessity and by establishing rights, obligations and sanctions. It is therefore inaccurate to say that digital privacy is legally unprotected in Algeria. Law No. 18-07 provides a foundation that can support a rights-based digital transformation.

Yet the protection remains incomplete. First, many individuals are not aware of their rights and therefore do not exercise them. Second, many institutions treat data protection as a formal requirement rather than as an ongoing compliance process. Third, the law needs practical guidelines adapted to sectors such as health, education, e-commerce, telecommunications and public administration. Fourth, the rapid development of artificial intelligence and profiling requires more precise rules on transparency, explainability and automated decision-making.

Consequently, the answer to the research question is nuanced. Algerian law has succeeded in establishing a necessary legal framework, but it has not yet achieved fully sufficient practical

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

protection for digital privacy. Adequate protection requires enforcement, awareness, institutional independence, technical expertise and continuous adaptation to technological change.

Conclusion

The right to privacy has evolved from the protection of private life in its traditional sense to the protection of personal data and digital identity. Digitalization has created new opportunities for communication, administration and economic activity, but it has also multiplied the risks of surveillance, profiling, unauthorized processing and data exploitation. In this context, digital privacy is no longer a secondary legal issue; it is a central condition for human dignity, autonomy and democratic participation.

The study shows that Algerian legislation, especially Law No. 18-07, has taken important steps toward protecting personal data. It recognizes essential principles such as consent, lawfulness, purpose limitation, information, access, rectification, objection, confidentiality, supervision and sanctions. These mechanisms provide a serious legal basis for protecting the right to digital privacy.

However, the article also concludes that the current framework is not fully sufficient in practice. The main challenge is not the total absence of legal rules, but the need to strengthen implementation, regulatory capacity, public awareness and adaptation to new technological risks. The comparison with the GDPR shows that Algeria can further develop its framework by clarifying breach notification duties, encouraging privacy by design, regulating automated decision-making, reinforcing accountability and improving the operational role of the National Authority.

Accordingly, the answer to the research question is that existing laws have partially succeeded in protecting the right to digital privacy. They provide an essential foundation, but they require stronger enforcement and modernization to ensure adequate protection in a rapidly changing digital environment.

Recommendations

1. Strengthen the independence, resources and technical capacity of the National Authority for the Protection of Personal Data.

2. Issue sector-specific guidelines for universities, health institutions, public administrations, banks, telecommunications operators and digital platforms.

3. Introduce clearer rules on data breach notification, data portability, privacy by design and automated decision-making.

4. Develop public awareness campaigns explaining the rights of information, access, rectification, objection and withdrawal of consent.

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

5. Require institutions that process sensitive data to conduct privacy impact assessments and maintain internal compliance documentation.

6. Promote digital literacy so that individuals understand the risks of excessive disclosure on social networks and digital platforms.

7. Encourage cooperation between Algerian regulators and international data protection authorities to address cross-border data flows.

References

Abou Bakr, O. M. (2004). Crimes arising from internet use: Substantive rules and procedural aspects. Dar Al-Nahda Al-Arabiya.

Al-Dosary, S. (2017). Living with privacy violation. Al-Sharq Al-Awsat Newspaper, 13981.

Al-Eidani, M. (2018). Protection of personal data in Algeria in light of Law 18/07. Malam Journal of Legal and Political Studies, 5.

Baji, A. (2020). Evolution of the concept of protecting the right to privacy. Law and Society Journal, 8(1).

Dahabi, K. (2017). The right to privacy in the face of electronic assaults. Journal of the Research Professor for Legal and Political Studies, 11(8).

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 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). Official Journal of the European Union, L119, 1-88.

Hamidani, S. (2019). Privacy breach in the digital world: Limits of the phenomenon and demands for legal protection. Journal of Research in Law and Political Science, 4(2).

Hezam, F. (2019). Legal guarantees for the processing of personal character data: A study in light of Law 18/07. Al-Ijtihad Journal for Legal and Economic Studies, 8(4).

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). 'It wouldn't happen to me': Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 143, Article 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Joudi, S. (2018). Legal protection of the right to information privacy. Al-Tawasul Journal, 24(2).

Karim, A. (2013). Digital privacy between violation and legislative absence. Marzou for IT Support.

Khalayfia, H. (2019). The internal and international legal framework for internet privacy protection. Series of Conference Proceedings on Privacy in the Information Society.

Khalfi, A. (2011). The right to private life in Algerian penal legislation. Journal of Research and Studies, 8(12).

Kirkitt, A. (2019). The right to privacy for users of digital space: Risks and challenges. Al-Haqiqa Journal of Social and Human Sciences, 18(2).

Vol. 06, No. 2, pp.468-477| JUNE 2026
DOI: https:// DOI 10.34118/jskp.v6i2.4654

Law No. 09-04 on the specific rules for the prevention of crimes related to information and communication technologies and their combat. (2009). Official Gazette of the Algerian Republic, 47.

Law No. 18-07 on the protection of natural persons in the field of processing personal character data. (2018). Official Gazette of the Algerian Republic, 34.

Mebarkia, M. (2018). Criminal protection of the right to digital privacy in Algerian law. Sharia and Economics Journal, 7(13).

Mohamed, M. N. (2010). Human rights to protect private life in international law and domestic legislation. Law and Economics Library.

Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. EMBO Reports, 19(8), Article e46579. https://doi.org/10.15252/embr.201846579

Seghir, J. A. B. (2000). The internet and criminal law. Dar Al-Nahda Al-Arabiya.

Tamam, A. H. T. (2000). Crimes arising from computer use. Dar Al-Nahda Al-Arabiya.

Zein Al-Abidin, M. (2016). International legal protection of personal data on the internet between international law and national law. Arab Studies Center.