



Protection of the Right to Privacy and Personal Data within the International Legal Framework

Bertal Abdelkader *

University of Laghouat
Law Research Laboratory and Society
Development
a.bertal@lagh-univ.dz

Received: 21/01 /2026

Accepted: 16/03 /2026

Published: 31/03 /2026

Abstract:

The right to privacy and personal data protection constitute fundamental pillars of human rights in the digital era. Beyond safeguarding individuals, they are essential for fostering trust and ensuring human dignity and freedoms. Despite international instruments such as the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966), rapid technological advancements, particularly in artificial intelligence and big data, reveal limitations in existing legal frameworks. This study examines the international legal protections, addressing challenges from cross-border data flows, multiple actors, and complex liability issues, highlighting that privacy protection is essential for rights and digital trust..

Keywords: Privacy, Protection of Personal Data, Human Rights, Digital Era, Legal Liability

Introduction

"The rapid digital transformation witnessed by the contemporary world has engendered a new legal reality that has reintroduced numerous traditional concepts of human rights into the forefront of legal discourse, most notably the right to privacy and the protection of personal data. In the digital age, privacy is no longer merely a narrow individual concern; rather, it has become an essential element for

* Corresponding author



fostering trust within the digital space and a fundamental pillar for safeguarding human dignity and basic freedoms, in light of the widespread prevalence of automated data processing and its cross-border flows".

"International human rights law has enshrined this right since its inception, notably through the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966), both of which codified the principle of non-interference against arbitrary or unlawful intrusion into the private lives of individuals. However, the remarkable acceleration in technological advancements, coupled with an unprecedented expansion in data collection, processing, and storage mechanisms, has clearly exposed the limitations of traditional legal frameworks in keeping pace with the profound transformations within the digital sphere. This issue has been further exacerbated by the transborder nature of data, widening the gap between existing legal instruments and the evolving digital reality, thereby rendering the international legal protection of privacy increasingly complex."

"Within this context, the international community confronts multifaceted legal challenges regarding the adequacy of the current international normative framework in ensuring effective privacy protection. This is exacerbated by the divergence of national legislations and the multiplicity of actors in the digital environment—including states, multinational corporations, and international organizations—as well as the interplay between national security considerations and the requirements for safeguarding fundamental rights and freedoms. This, in turn, raises fundamental questions concerning the scope of state obligations, the dilemma of legal liability, and the resilience of existing international rules in keeping pace with rapid digital transformations.

Consequently, the central problem of this intervention revolves around the efficacy of the established international legal framework in protecting the right to privacy and personal data within the digital sphere, and the limitations of this framework in addressing challenges arising from transborder data flows in the absence of a unified and comprehensive international instrument."

"To address this problematic, this intervention employs a critical analytical methodology by examining relevant international legal instruments, while highlighting the practical lacunae that impede the realization of effective privacy protection at the international level.

Accordingly, this research paper is structured into two primary thematic axes: The first axis explores the international legal framework for the protection of



privacy and personal data within the digital environment; whereas the second axis is dedicated to analyzing the most salient international legal challenges confronting such protection, particularly in light of the transborder nature of data and the multiplicity of actors within the digital sphere."

"Section I: International Treaty-Based Efforts for the Protection of Personal Data"

The right to privacy and the protection of personal data constitute fundamental pillars of the human rights regime. These rights have been enshrined by international law through various UN instruments and conventions designed to safeguard individuals within the digital era. Moreover, regional conventions and legislative frameworks—notably the Council of Europe Convention 108 and the General Data Protection Regulation (GDPR)—have been instrumental in setting forth definitive standards for transparency and accountability."

1. "UN Efforts in Safeguarding Privacy and the Protection of Personal Data"

Legal jurisprudence holds a consensus that the right to privacy is no longer an intellectual luxury or a mere moral value; rather, it constitutes the bedrock of any society that respects human dignity. This principle has been enshrined in international human rights law since the mid-twentieth century. The Universal Declaration of Human Rights (1948) affirmed, in its Article 12, that the private lives of individuals shall be immune from any arbitrary interference.¹

"Nevertheless, the substantive legal force of this principle only materialized with the adoption of the International Covenant on Civil and Political Rights (1966). This instrument elevated the right to privacy from a mere moral proclamation into a binding legal obligation, the breach of which triggers the international responsibility of States²

However, with the evolution of digital technology, new challenges have emerged, rendering traditional legal frameworks inadequate to address them. Interference with privacy is no longer confined to direct espionage or physical surveillance; it has morphed into more sophisticated forms associated with Big Data harvesting and its analysis via Artificial Intelligence (AI) algorithms. These algorithms do not merely track individual behavior but seek to predict future conduct—a practice which the UN General Assembly, in its 2014 resolution,

1 United Nations, Universal Declaration of Human Rights, 1948, Art. 12."

2 United Nations, International Covenant on Civil and Political Rights, 1966, Art. 17.



characterized as a manifest threat to individual liberty and a range of other rights, most notably the rights to freedom of expression and peaceful assembly¹

"The situation is further exacerbated by the fact that AI technologies frequently operate as 'black boxes'—that is, without a transparent understanding of the underlying decision-making logic. This prompted the Human Rights Council (2018) to emphasize that the opacity and lack of accountability in this domain facilitate arbitrary practices that are inherently difficult to detect or judicially contest²

On the other hand, the international community confronts a formidable dilemma arising from the transborder nature of technology. While international law establishes overarching principles for privacy protection, their operative implementation remains contingent upon disparate national legislations. This fragmentation occasionally enables multinational corporations to exploit legal loopholes in jurisdictions with lax oversight.

Many experts contend that cross-border data flows constitute the preeminent challenge to the international legal order, as they undermine the efficacy of domestic protections in the absence of binding international instruments that harmonize rules and bridge existing gaps³ Consequently, privacy protection in the AI era has shifted from a conventional human rights discourse into a fundamental tension between the imperatives of innovation and the preservation of core human rights values.

2. "The General Data Protection Regulation (GDPR) and its Impact as a Transborder International Standard

The General Data Protection Regulation (GDPR) is widely regarded⁴ as the most pivotal legal instrument in the modern history of data protection. Notwithstanding its nature as a regional legislation, its 'universal' character stems

1 United Nations, General Assembly, The Right to Privacy in the Digital Age, Resolution A/RES/69/166, 2014.

2 UN Human Rights Council, The Right to Privacy in the Digital Age, Report A/HRC/39/29, 2018.

3 Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, p. 141.

4 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679): Was adopted by the European Parliament and the Council of the European Union on April 27, 2016, and officially entered into force on May 25, 2018, superseding the Data Protection Directive 95/46/EC. It aims to harmonize data privacy laws across the EU, empower individuals' data rights, and institutionalize the principles of transparency and accountability. A defining feature of the GDPR is its extraterritorial scope (Extraterritoriality), as it applies to any global entity processing the personal data of individuals located within the EU, irrespective of the entity's physical jurisdiction."



from its extraterritorial application, imposing stringent protection standards on any data controller or processor worldwide that handles the personal data of European citizens.

This Regulation has established imperative international principles, most notably 'transparency' and 'purpose limitation', while introducing innovative digital rights such as the 'right to data portability' and the 'right to be forgotten'. Furthermore, the legal significance of the GDPR lies in its capacity to harmonize substantive rules of protection, thereby mitigating the phenomenon of 'data havens' previously exploited by multinational corporations to evade legal liability."

"Furthermore, the Council of Europe Convention 108 (1981) constitutes the first binding international instrument dedicated to the protection of individuals against risks arising from the automatic processing of personal data. The Convention established a set of core principles, notably the lawfulness of data collection and processing—including purpose specification, accuracy and adequacy, and the limitation of data retention periods. Additionally, it enshrined fundamental data subject rights, such as the rights of access, rectification, and erasure, as well as the right to object to processing. The Convention also prohibited the processing of sensitive categories of data—such as racial origin, religious or political beliefs, health, and sexual life—except where provided by clear legal safeguards¹

However, the rapid technological advancements—spanning from the information revolution to the advent of Artificial Intelligence and Big Data analytics—exposed the limitations of the Convention's original provisions. Consequently, the 2018 Amending Protocol (Convention 108+) emerged as a vital step toward modernizing the legal framework. This update reinforced the principles of transparency and accountability, introducing novel mechanisms such as data breach notification, data minimization, and the obligation for States to establish independent national supervisory authorities vested with regulatory and investigative powers. Furthermore, it expanded data subject rights to include the right to object, restriction of processing, and the right to challenge automated decisions²

1 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Strasbourg, 28 January 1981, Articles 5–8."

2 Al-Salihin Mohammed Al-Aish, Protection of Personal Data in European Law, Kuwait International Law School Journal, Issue 3, 2023, p. [insert page number]."



"These updates have brought Convention 108+ into close alignment with the General Data Protection Regulation (GDPR), which was adopted by the European Union in 2016 and entered into force in 2018. The GDPR constitutes the most comprehensive and robust regional framework for personal data protection to date. It enshrines analogous fundamental principles, such as lawfulness, transparency, and data minimization, while bolstering data subject rights—including data portability, the right to be forgotten, and the right to object to automated decision-making. Furthermore, the Regulation introduced a stringent administrative sanctions regime, imposing fines that can reach a significant percentage of a corporation's total global annual turnover¹

While the GDPR remains a binding regional framework within the European Union, the distinctive advantage of Convention 108+ resides in its international dimension. By facilitating the accession of non-European states—as evidenced by Tunisia's joining in 2017—it has acquired a global normative character that bolsters digital trust and fosters international legislative convergence in privacy protection. The synergy between the GDPR, as a rigorous regional benchmark, and Convention 108+, as a flexible international reference, paves the way for an integrated legal order that balances the free flow of transborder data with the protection of fundamental privacy rights. This evolution serves as a necessary response to contemporary challenges, such as e-commerce and Artificial Intelligence, which have established privacy protection as a pivotal cornerstone of digital trust."

3."Digital Trade Law Initiatives and the Limitations of International Privacy Protection

Although international efforts in digital trade law represented an initial step toward the recognition of electronic transactions and the consolidation of digital trust, these endeavors have revealed a notable deficiency regarding the protection of personal data. The initiatives of the United Nations Commission on International Trade Law (UNCITRAL), such as the Model Law on Electronic Commerce (1996)² and the Model Law on Electronic Signatures (2001), were developed primarily to facilitate cross-border commercial exchanges and ensure the legal validity of electronic instruments. However, they failed to prescribe specific normative rules for privacy safeguarding or to address the complex legal challenges arising from transborder data flows³

1 uca Bertoni, Convention 108 and the GDPR, Privacy + Security Academy, 2020, p. 3."

2 UNCITRAL, Model Law on Electronic Commerce, 1996

3 UNCITRAL, Model Law on Electronic Signatures, 2001



"This dichotomy is not merely limited to the conflict of laws between sovereign states; it further encompasses the friction between data protection regimes and other legal domains, such as national security mandates and international trade regulations. This underscores the imperative for a comprehensive global framework, as national or regional instruments—irrespective of their normative sophistication—prove insufficient against the fluid nature of data, which operates within a borderless digital sphere that transcends geographical jurisdictions¹

"Consequently, it can be asserted that while the UNCITRAL Model Laws were instrumental in laying the legal groundwork for electronic transactions, they remain ill-equipped to tackle the contemporary challenges necessitated by Artificial Intelligence and global data streams. Hence, it has become imperative to transition from the phase of piecemeal initiatives toward a comprehensive and binding international convention. Such a treaty must encapsulate modern technological intricacies and strike a judicious balance between the exigencies of innovation and the preservation of fundamental individual rights."

"Section II: International Legal Challenges to Personal Data Protection

Notwithstanding the international and regional endeavors to institute legal frameworks for personal data protection, the current digital reality uncovers **profound lacunae** that undermine the **legal efficacy** of such protections—most notably amidst the **pervasive expansion** of Artificial Intelligence. These paramount challenges can be delineated across three fundamental levels:"

1. "The Absence of a Unified International Legal Framework for Regulating Transborder Data Flows

International data protection law suffers from 'regulatory fragmentation.' While the European Union possesses a stringent framework, numerous states still lack a comprehensive legislative umbrella. This disparity creates 'protection gaps' within transborder flows. The absence of a 'universal convention' under the auspices of the United Nations—prescribing unified minimum standards—complicates international judicial cooperation in data-related crimes. It further exacerbates the tension between the 'free flow of data' necessary for digital trade and the 'data sovereignty' of individuals—a legal conflict that the international community has yet to resolve definitively.

1 Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, p. 141



This lack of a unified global framework is not merely a formalistic matter; rather, it constitutes a structural problematic within the international legal order. Existing initiatives, such as Convention 108, despite their historical significance as the inaugural international instruments in this field, remain largely confined to a regional jurisdiction. They have not ascended to the status of a binding universal treaty, notwithstanding the accession of several non-European states to the amended version. This regional limitation was further underscored by the UNCTAD report, which emphasized that most national frameworks lack interoperability. This misalignment renders international data flows susceptible to regulatory hurdles that impede e-commerce and digital development in developing nations¹

Legal jurisprudence has further observed that this fragmentation among national legislations engenders a phenomenon akin to a 'conflict of laws.' This occurs as sovereign states endeavor to assert the extraterritorial application of their domestic regulations over data, even when such data is processed beyond their borders. This practice creates a sharp friction between disparate legal systems and ultimately leads to the erosion of legal protections for privacy at the international level²

On a practical level, the OECD has underscored that relying on mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) remains a partial remedy that fails to address the root of the problem. These instruments are primarily predicated on party autonomy and lack international enforcement power; moreover, they offer inadequate safeguards against gross infringements perpetrated by external actors.³

In a similar vein, the experience of the African Union—exemplified by the Malabo Convention on Cyber Security and Personal Data Protection—demonstrates that the lack of legislative harmonization among member states obstructs the uniform application of the convention, rendering it incapable of countering the transborder challenges of modern technology⁴

1 UNCTAD, Data Protection Frameworks Must Be Compatible with International Data Flows, Press Release, 2016."

2 Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press, 2013, Chapters 6 & 8.

3 OECD, Report on Transborder Data Flow Contracts within the Wider Framework of Privacy Protection Mechanisms on Global Networks, available at: <https://www.oecd.org>.

4 African Union, Convention on Cyber Security and Personal Data Protection: Challenges and Future Prospects, 2023, available at: <https://arxiv.org/abs/2307.01966>.



Consequently, the absence of a unified global legal framework does not merely create protection gaps but also poses a sovereignty problematic. States increasingly prioritize national interests over the establishment of an equitable international legal order. This results in political ramifications, notably the emergence of 'digital spheres of influence' where major powers impose their own standards: (the EU through the GDPR, the US through a market-centric model, and China through a centralized surveillance model). This deepens the divide, rendering individual rights contingent upon geographical jurisdiction rather than being upheld as universal rights."

"Consequently, the absence of a unified global legal framework does not merely create protection gaps but also poses a sovereignty problematic. States increasingly prioritize national interests over the establishment of an equitable international legal order. This results in significant political ramifications, notably the emergence of 'digital spheres of influence' where major powers impose their own idiosyncratic standards: the European Union via the GDPR, the United States through a market-driven model, and China through a centralized surveillance paradigm. Such fragmentation deepens the divide, rendering individual rights contingent upon geographical jurisdiction rather than being upheld as universal, inalienable rights."

2."Legal Liability in the Big Data and Artificial Intelligence Environment

The issue of legal liability represents one of the most intricate challenges in the field of data protection within the AI era. The nature of algorithms—predicated on massive processing and autonomous learning—renders it difficult to identify the party directly liable for damages arising from data breaches or unlawful processing. In response, the General Data Protection Regulation (GDPR) has adopted an approach that holds the 'Data Controller' primarily responsible for adhering to the principles of lawfulness and transparency, and for ensuring the protection of individuals' rights. This reinforces the principle of accountability as one of the central pillars of legal protection

"Nevertheless, this mechanism remains limited in the face of the technical complexity of intelligent systems and the inherent nature of transborder data flows. Christopher Kuner contends that liability cannot be restricted to national actors alone; the transnational nature of data leads to a conflict of laws and a divergence of legal regimes. This necessitates the formulation of clearer international rules for



the apportionment of liability among the various stakeholders in the digital ecosystem¹

3."Human Rights Implications and Digital Sovereignty Challenges in Privacy Protection

Privacy constitutes a fundamental pillar of the human rights system. The International Covenant on Civil and Political Rights (ICCPR) of 1966 explicitly stipulates in Article 17 that no one shall be subjected to arbitrary or unlawful interference with their privacy or correspondence. However, technological advancements—characterized by the pervasive reliance on Artificial Intelligence and Big Data processing—have catalyzed new legal dilemmas. On one hand, the question of balancing rights emerges: how can innovation and the digital economy be fostered without undermining the right to privacy? On the other hand, the challenge of fragmented authority arises; data protection is now a domain shared by private corporations, national regulators, and international organizations, complicating the identification of the liable party in cases of data breaches. Furthermore, from a security perspective, many states justify the surveillance of personal data under the pretext of counter-terrorism or national security. Yet, such practices pose an explicit threat to privacy unless circumscribed by effective legal safeguards. In this context, the European legislator, through the General Data Protection Regulation (GDPR) of 2016,² sought to establish balanced mechanisms to protect individual privacy—such as the principle of proportionality and the right to object to processing. Nevertheless, these safeguards continue to encounter practical hurdles, primarily the difficulty of imposing transparency on complex technical systems."

Conclusion

In conclusion, it is evident that the protection of personal data in the era of Artificial Intelligence has transcended being a merely technical or regulatory matter; it is now a fundamental issue directly impacting human rights. Technological advancements have significantly accelerated the velocity and complexity of data processing and analytics, raising profound questions regarding individual privacy and the legal liability of those who control such data.

Despite the existence of pivotal legal instruments—such as Convention 108+ and the GDPR—these frameworks alone are insufficient to address transborder digital flows and autonomous systems operating within 'black boxes,' where the

1 Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, previously cited, Chapters 6 & 8."

2 General Data Protection Regulation (GDPR), *supra* note



underlying logic of decision-making remains opaque. Furthermore, the legislative divergence among states exacerbates these complexities, rendering privacy protection inconsistent across different jurisdictions.

Consequently, a concerted international effort is required to establish clear and equitable standards that safeguard individuals, define liabilities, and institutionalize transparency and accountability. It is imperative for states to cooperate to ensure that data protection is no longer contingent upon geographical jurisdiction, but rather upheld as a universal right for every digital user, regardless of their location."

References & Bibliography

I. International Documents & Resolutions

1. United Nations. (1948). Universal Declaration of Human Rights.
2. United Nations. (1966). International Covenant on Civil and Political Rights (ICCPR).
3. United Nations General Assembly. (2014). The Right to Privacy in the Digital Age. Resolution A/RES/69/166.
4. United Nations Human Rights Council. (2018). Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age. Document A/HRC/39/29.
5. United Nations Commission on International Trade Law (UNCITRAL). (1996). UNCITRAL Model Law on Electronic Commerce.
6. United Nations Commission on International Trade Law (UNCITRAL). (2001). UNCITRAL Model Law on Electronic Signatures.
7. United Nations Conference on Trade and Development (UNCTAD). (2016). Data Protection Regulations and International Data Flows: Implications for Trade and Development.

II. Regional Conventions & Legislation

8. European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679, Official Journal of the European Union (OJ).



9. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), and its Amending Protocol (Convention 108+).

10. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

11. Organisation for Economic Co-operation and Development (OECD). (2020). Report on Cross-border Data Flow Contracts and Privacy Protection Mechanisms.

III. Books & Scholarly Articles

12. Kuner, C. (2013). Transborder Data Flows and Data Privacy Law. Oxford University Press.

13. Bertoni, U. (2020). Convention 108 and the GDPR: A Comparative Analysis. Privacy + Security Academy.

14. Al-Salihin, M. (2023). "Personal Data Protection in European Law." Kuwait International Law School Journal (KILAW), Issue No. 3.