
Personal data protection and digital privacy: regulation, rights and challenges in contemporary technological environments

Protección de datos personales y privacidad digital: regulación, derechos y desafíos en entornos tecnológicos contemporáneos

Proteção de dados pessoais e privacidade digital: regulação, direitos e desafios nos ambientes tecnológicos contemporâneos.

Tahiri Saad

✉ : tahirisaad80@gmail.com

id : <https://orcid.org/0009-0001-5075-8077>

Universidad Ziane Achour de Djelfa, Algeria

Cita sugerida (APA, séptima edición)

Saad, T. (2026). Personal data protection and digital privacy: regulation, rights and challenges in contemporary technological environments. *Tribunal de Justicia, Revista de Investigación jurídica*. 3(2), 92-106. DOI: <https://doi.org/10.51247/tj.v3i2.973>

Abstract

This article aimed to analyze the legal regulation of personal data protection and examine the main challenges facing digital privacy in contemporary technological environments, considering the regulatory, doctrinal, and technological evolution that characterizes the information society. The study was conducted using a qualitative approach through a systematic review with a narrative scope. Scientific publications, specialized legal doctrine, national and international legislation, and relevant legal instruments were collected and analyzed according to criteria of relevance, recency, academic impact, and consistency with the research objectives. The findings showed that personal data protection has become an autonomous fundamental right supported by principles such as legality, consent, purpose limitation, proportionality, and security. Furthermore, the study identified that the expansion of big data, artificial intelligence, digital surveillance, and cybersecurity threats has increased the risks to individual privacy, requiring adaptive regulatory frameworks and stronger supervisory mechanisms. It is concluded that personal data protection represents a fundamental pillar of digital governance and demands continuous regulatory updating, institutional strengthening, and international cooperation to ensure an appropriate balance between technological innovation, digital development, and the effective protection of fundamental rights.

Keywords: personal data protection; digital privacy; digital rights; legal regulation.

Resumen

El presente artículo tuvo como objetivo analizar la regulación jurídica de la protección de datos personales y examinar los principales desafíos que enfrenta la privacidad digital en los entornos tecnológicos contemporáneos, considerando la evolución normativa, doctrinal y tecnológica que caracteriza a la sociedad de la información. La investigación se desarrolló mediante un enfoque cualitativo bajo la modalidad de revisión sistemática con alcance narrativo. Para ello, se recopilaron y analizaron publicaciones científicas, doctrina especializada, legislación nacional e internacional e instrumentos jurídicos relevantes, seleccionados conforme a criterios de actualidad, pertinencia, impacto académico y relación con el objeto de estudio. Los resultados evidenciaron que la protección de los datos personales se ha consolidado como un derecho fundamental autónomo sustentado en principios como la legalidad, el consentimiento, la finalidad, la proporcionalidad y la seguridad. Asimismo, se identificó que el crecimiento del big data, la inteligencia artificial, la vigilancia digital y las amenazas a la ciberseguridad incrementan los riesgos para la privacidad, exigiendo marcos regulatorios dinámicos y mecanismos efectivos de supervisión. Se concluye que la protección de los datos personales constituye un componente esencial de la gobernanza digital y requiere la actualización permanente de la normativa, el fortalecimiento institucional y la cooperación internacional para garantizar el equilibrio entre innovación tecnológica, desarrollo digital y respeto efectivo de los derechos fundamentales.

Palabras clave: protección de datos personales; privacidad digital; derechos digitales; regulación jurídica.

Resumo

O presente artigo teve como objetivo analisar a regulamentação jurídica da proteção de dados pessoais e examinar os principais desafios enfrentados pela privacidade digital nos ambientes tecnológicos contemporâneos, considerando a evolução normativa, doutrinária e tecnológica própria da sociedade da informação. A pesquisa foi desenvolvida por meio de uma abordagem qualitativa, utilizando uma revisão sistemática com alcance narrativo. Foram selecionados e analisados artigos científicos, doutrina especializada, legislação nacional e internacional e instrumentos jurídicos relevantes, de acordo com critérios de atualidade, pertinência, impacto acadêmico e relação com o objeto de estudo. Os resultados evidenciaram que a proteção de dados pessoais consolidou-se como um direito fundamental autônomo, fundamentado nos princípios da legalidade, do consentimento, da finalidade, da proporcionalidade e da segurança. Também foi identificado que o crescimento do big data, da inteligência artificial, da vigilância digital e das ameaças à cibersegurança ampliou significativamente os riscos à privacidade, exigindo estruturas regulatórias mais dinâmicas e mecanismos eficazes de fiscalização. Conclui-se que a proteção de dados pessoais constitui um elemento essencial da governança digital e requer atualização permanente da legislação, fortalecimento institucional e cooperação internacional para assegurar o equilíbrio entre inovação tecnológica, desenvolvimento digital e proteção efetiva dos direitos fundamentais.

Palavras-chave: proteção de dados pessoais; privacidade digital; direitos digitais; regulação jurídica.

Introduction

The protection of personal data and digital privacy constitutes one of the main challenges of contemporary law due to the expansion of information technologies, global connectivity, and the massive processing of personal information. The development of digital environments has profoundly transformed the way individuals interact, work, consume, and exercise their

fundamental rights, generating new scenarios that require effective legal responses. Within this context, privacy is no longer understood solely as a sphere of private life but rather as a right closely associated with human dignity, personal autonomy, and individual freedom, aspects that demand protection mechanisms consistent with the current technological reality.

The evolution of the right to privacy has responded to the social and technological transformations experienced over recent decades. In its initial formulations, this right was primarily focused on protecting individuals' intimate sphere against arbitrary interference by the State or private actors. However, the expansion of digital systems, the computerization of public and private services, and the continuous circulation of information on the Internet have considerably broadened the scope of legal protection. In this regard, Talciani (1999) argues that privacy constitutes an essential prerequisite for the free development of personality, as it guarantees spaces of autonomy where individuals can exercise their rights without undue interference.

The consolidation of the digital society has generated new dimensions of the right to privacy that transcend the individual protection of personal data. The use of algorithms, artificial intelligence systems, and predictive analytics mechanisms enables the creation of collective profiles that simultaneously affect groups of individuals, even when there is no direct identification of each person. From this perspective, Castillo Parrilla (2023) explains that group privacy represents one of the greatest challenges for contemporary law, since intelligent technologies can infer sensitive characteristics through large-scale data processing, significantly increasing risks to fundamental rights.

The regulatory evolution has also been influenced by the incorporation of international standards aimed at strengthening the protection of personal data as a human right. Several countries have developed legal frameworks based on principles such as lawfulness, transparency, proportionality, purpose limitation, and accountability in the processing of information. Regarding the Colombian case, Rojas-Bejarano (2014) highlights that the harmonization with international standards contributed to consolidating legal mechanisms aimed at ensuring higher levels of protection against risks arising from automated processing of personal information, thereby reinforcing the principle of informational self-determination.

At the same time, the rapid development of digital technologies has generated significant benefits for education, the economy, electronic commerce, and public administration. Digitalization facilitates access to knowledge, optimizes productive processes, and improves the provision of multiple services through intelligent platforms. In the educational field, Zambrano Mera and Chancay García (2024) indicate that digital technologies promote more dynamic, collaborative, and interactive teaching and learning processes, expanding access to information and strengthening the digital competencies of students and educators.

In the economic sphere, digital transformation has profoundly reshaped international commercial relations through electronic platforms, artificial intelligence, data analytics, and cross-border digital services. These tools enhance business competitiveness and enable new forms of economic exchange; however, they also intensify the continuous collection of information regarding consumers, suppliers, and users. In this regard, García (2019) states that the digital economy increasingly relies on intensive data processing as a strategic resource for innovation, productivity, and business decision-making.

Nevertheless, the extensive use of digital technologies has also increased the risks associated with the massive exploitation of personal data. Currently, governments, technology companies, financial institutions, digital platforms, and social networks collect vast amounts of information that are subsequently used for commercial, statistical, advertising, or surveillance purposes. This reality raises significant questions regarding the limits of data processing and the ability of individuals to effectively control their personal information within highly complex digital ecosystems.

In this scenario, Martínez Devia (2019) warns that the convergence of artificial intelligence, big data, and automation represents a significant threat to personal data protection due to the enormous technological capacity to collect, store, combine, and analyze information obtained from multiple sources. Likewise, González Guerrero (2019) demonstrates that web tracking carried out by third parties enables the construction of detailed user profiles through continuous monitoring techniques, considerably reducing individuals' effective control over their own data on the Internet.

Given this reality, legal protection acquires strategic importance in ensuring a balance between technological innovation and the safeguarding of fundamental rights. New regulatory frameworks seek to strengthen principles such as informed consent, transparency, data minimization, accountability of data controllers, and the effective exercise of rights related to access, rectification, erasure, and objection. According to Arellano López (2020), the right to personal data protection currently constitutes an autonomous guarantee that preserves individual freedom against the indiscriminate use of personal information in the digital society.

In the Ecuadorian context, the enactment of the Organic Law on Personal Data Protection represents a significant advancement in consolidating the right to informational self-determination and adapting the legal system to international standards. Cordero Alemán (2023) argues that this regulation strengthens the habeas data mechanism and establishes specific obligations for those responsible for personal data processing, promoting greater legal certainty for both citizens and public and private organizations.

Within this framework, this article aims to analyze the legal regulation of personal data protection and examine the main challenges faced by digital privacy in contemporary technological environments. To achieve this purpose, the study addresses the following research questions: How is personal data protection currently regulated in response to technological advances? What are the main challenges confronting digital privacy in a context characterized by massive data utilization, artificial intelligence, and digital transformation? Answering these questions will contribute to understanding existing regulatory developments, identifying the main tensions between technological innovation and fundamental rights, and providing elements for strengthening public policies aimed at ensuring effective privacy protection in the digital era.

Methodology

This study was conducted using a qualitative research approach, which is particularly suitable for examining and interpreting legal phenomena related to personal data protection and digital privacy in contemporary technological environments. A systematic review with a narrative scope was adopted, as it enabled the identification, organization, critical analysis, and integration of the principal doctrinal, normative, and scientific contributions concerning the regulation of personal data, digital rights, and the legal challenges arising from ongoing technological transformation. According to Anticona et al. (2023), this type of research facilitates the critical synthesis of existing knowledge through systematic processes of evidence identification, selection, comparison, and interpretation.

The documentary review was conducted through a comprehensive search of specialized scientific literature, including articles published in indexed academic journals, scholarly books, postgraduate theses, national and international legal instruments, and technical reports issued by organizations specializing in personal data protection. The selection of documentary sources was based on previously established criteria, including thematic relevance, publication currency, scientific rigor, academic impact, and direct alignment with the objectives of the study. Furthermore, documentary sources were examined critically and responsibly, following the methodological recommendations for legal research proposed by Botero Bernal (2016).

Subsequently, the collected information was subjected to doctrinal, normative, and comparative legal analysis. The doctrinal analysis made it possible to identify the principal theoretical approaches concerning the right to privacy, informational self-determination, and personal data protection. The normative analysis examined the main legal instruments governing personal data protection, while the comparative analysis facilitated the identification of similarities, differences, and emerging regulatory trends across different legal systems. In this regard, Avellaneda Vásquez (2024) argues that contemporary legal research requires the integration of interdisciplinary perspectives capable of explaining the evolution of legal systems in response to rapid social and technological change.

Throughout the research process, the study adhered to the ethical principles governing qualitative legal research. Proper acknowledgment of authorship was ensured through the consistent application of APA citation and referencing standards, the intellectual integrity of all consulted sources was respected, and the interpretation of the evidence was carried out objectively to minimize potential bias that could compromise the validity of the findings. In line with Parra Domínguez and Briceño Rodríguez (2013), research ethics constitutes a fundamental component for ensuring the credibility, transparency, and trustworthiness of the scientific process and the conclusions derived from it.

Development

Personal Data and Privacy: Conceptual Foundations

The protection of personal data has become one of the fundamental pillars of contemporary digital law, as information relating to individuals has acquired strategic value across economic, social, political, and technological domains. The rapid expansion of the Internet, the digitalization of public and private services, and the development of intelligent digital platforms have transformed personal data into a critical resource for automated decision-making, thereby increasing the need for legal mechanisms capable of safeguarding fundamental rights. Within this context, legal scholarship has evolved from a traditional understanding of privacy toward a comprehensive framework for the protection of personal information as an expression of human dignity.

From a legal perspective, personal data encompass any information that identifies or can render a natural person identifiable, either directly or indirectly. This definition includes identification data, biometric information, financial records, health-related information, geolocation data, IP addresses, consumer behavior, and any other element capable of being associated with an individual. Conde Ortiz (2005) argues that the protection of personal data constitutes an autonomous fundamental right, distinct from the right to privacy, because its primary objective is to ensure that individuals retain control over the use of their personal information, regardless of whether such information belongs to the strictly private sphere.

The evolution of legal doctrine demonstrates that the concept of privacy has undergone profound transformations as a consequence of technological advancement. Whereas early legal approaches primarily focused on protecting individuals' private lives against external interference, contemporary concerns increasingly revolve around the automated processing of information and the extensive power exercised by public and private organizations to collect, store, and analyze vast amounts of personal data. López-Torres (2014) explains that the development of the international legal framework for data protection emerged precisely from the need to establish effective legal safeguards against the rapid expansion of information technologies and the growing cross-border exchange of personal information.

The widespread adoption of the Internet has considerably amplified privacy-related risks. Constant device connectivity, social networking platforms, mobile applications, and cloud-based services generate continuous flows of personal information that frequently remain

beyond the knowledge and effective control of users themselves. Drummond (2004) anticipated that the architecture of the Internet would fundamentally reshape the understanding of privacy by facilitating the unlimited reproduction, storage, and dissemination of personal information through increasingly sophisticated technological tools.

Current legal scholarship broadly recognizes that privacy, private life, and personal data protection are closely interconnected yet legally distinct rights. While privacy safeguards the sphere of individual autonomy, personal data protection specifically regulates the conditions under which identifiable information may be processed by third parties. Maqueo Ramírez et al. (2017) argue that the principal contemporary challenge lies in achieving a global balance between technological innovation, digital transformation, and the effective protection of fundamental rights, ensuring that the large-scale circulation of personal information does not undermine individual freedom.

Empirical studies conducted throughout Latin America reveal that a significant proportion of the population remains unaware of the extent to which their personal information is collected, processed, and exploited within digital ecosystems. This lack of awareness increases individuals' vulnerability to intrusive commercial practices, automated profiling, and technological surveillance mechanisms. In a study conducted in Costa Rica, Rivera Barrantes (2019) concluded that public perceptions regarding privacy remain limited, particularly concerning the use of personal information by digital platforms and technology companies, highlighting the urgent need to strengthen both legal regulation and digital literacy simultaneously.

Principles of Personal Data Protection

The principles governing personal data protection constitute the structural foundation of legal systems designed to ensure the responsible processing of personal information. These principles guide the conduct of both public institutions and private organizations involved in collecting, storing, or managing personal data, while also providing the interpretative framework for the obligations established by applicable legislation. Their significance lies in establishing general legal standards that constrain technological power and safeguard fundamental rights within societies increasingly characterized by large-scale data processing.

Among these principles, the principle of lawfulness occupies a central position, requiring that all processing of personal data be grounded in a valid legal basis and conducted within the limits established by applicable legislation. This principle prevents arbitrary data collection and requires that all processing activities pursue legitimate and previously specified purposes. Martínez (2007) argues that personal data protection attained the status of a fundamental right precisely because it imposes legal constraints on automated information processing, thereby reinforcing the balance between technological development and the protection of individual rights.

Consent represents another essential principle of personal data protection. Its purpose is to ensure that data subjects retain effective control over the use of their information through a freely given, specific, informed, and unambiguous expression of will. However, the rapid expansion of digital platforms has exposed significant practical limitations affecting the effectiveness of this mechanism, primarily due to the complexity of privacy policies and the substantial asymmetries of information and bargaining power between users and technology service providers. Porcelli (2019) observes that Ibero-American regulatory standards have progressively evolved toward models that strengthen informed consent while simultaneously expanding the transparency obligations imposed upon data controllers.

Equally significant is the principle of purpose limitation, according to which personal data may only be collected for specific, explicit, and legitimate purposes, thereby preventing their subsequent use for objectives incompatible with those that originally justified their collection.

This principle is closely linked to the principle of proportionality, which requires limiting data collection exclusively to information that is strictly necessary for achieving the declared purpose. Pouillet and Dinant (2007) argue that the contemporary digital environment requires a reinterpretation of these traditional principles because emerging technologies increasingly enable the reuse of personal information for purposes that were originally unforeseeable.

Finally, the principle of security requires data controllers to implement appropriate technical, organizational, and legal measures designed to protect personal information against unauthorized access, loss, alteration, destruction, or unlawful disclosure. Security has evolved beyond being merely a technological requirement to become a continuous legal obligation, particularly in response to the growing incidence of cyberattacks and large-scale data breaches. Within this context, Cano (2012) emphasizes that strengthening information security policies constitutes one of the greatest challenges facing Latin American personal data protection systems, given the accelerated expansion of digital services and the increasing sophistication of cybersecurity threats.

Rights of Personal Data Subjects

The consolidation of the fundamental right to personal data protection is materialized through the recognition of a set of legal entitlements that enable data subjects to exercise effective control over information relating to them. These rights reinforce the principle of informational self-determination by granting individuals the ability to access, modify, restrict, or prevent specific processing activities whenever such processing infringes their rights or exceeds the purposes authorized by applicable law.

Among the most significant rights is the right of access, through which every individual is entitled to ascertain whether their personal data are being processed, identify the data controller, and obtain information concerning the purposes of processing, categories of personal data, recipients, and applicable retention periods. This right constitutes the cornerstone of all other data protection mechanisms because it ensures transparency in the management of personal information. Porcelli (2019) emphasizes that international data protection standards recognize the right of access as an indispensable prerequisite for strengthening public trust in digital ecosystems.

Complementing this guarantee are the rights of rectification, erasure, and objection, commonly referred to within Ibero-American legal systems as the ARCO rights. The right to rectification enables individuals to correct inaccurate or incomplete information; the right to erasure allows them to request the deletion of personal data that are no longer necessary or have been processed unlawfully; and the right to object empowers data subjects to oppose specific processing activities based on legitimate grounds relating to their particular circumstances. Bordachar Benoit (2022) warns that several Latin American legislative initiatives continue to exhibit technical shortcomings regarding the effective regulation of these rights, particularly in the context of automated data processing.

Technological innovation has also fostered the recognition of the **right to data portability**, which allows individuals to obtain their personal information in structured, commonly used, and interoperable formats for transmission between different digital service providers. This right promotes market competition, facilitates users' freedom to choose digital platforms, and mitigates the effects of technological lock-in. Simultaneously, the increasing internationalization of data flows requires effective mechanisms for regulating cross-border data transfers and ensuring consistent levels of legal protection across jurisdictions. Giménez, Real, and García (2015) argue that unlawful international data transfers constitute one of the principal sources of vulnerability for data subjects when personal information is transferred to jurisdictions lacking adequate regulatory safeguards.

From a critical perspective, contemporary legal scholarship maintains that the effective exercise of data subject rights continues to encounter significant challenges arising from technological complexity, algorithmic opacity, and the concentration of personal information within large digital platforms. In the Ecuadorian context, Roldán Carrillo (2021) argues that both consent and purpose limitation should be reinforced through more rigorous regulatory mechanisms capable of ensuring the meaningful exercise of data subject rights in response to the increasing deployment of artificial intelligence, big data analytics, and automated decision-making systems. Consequently, the current state of legal scholarship demonstrates that the effectiveness of the rights recognized by data protection legislation depends not only on their formal legal recognition but also on the existence of independent supervisory authorities, efficient administrative enforcement mechanisms, and a societal culture committed to safeguarding digital privacy.

Legal Framework for Personal Data Protection

The consolidation of the right to personal data protection has been accompanied by significant legislative development at both the national and international levels. The rapid expansion of digital services, the increasing volume of cross-border data transfers, and the widespread adoption of artificial intelligence technologies have stimulated the enactment of legal instruments designed to ensure the lawful, transparent, and secure processing of personal information. Consequently, contemporary legal systems have progressively incorporated principles, obligations, and supervisory mechanisms aimed at strengthening the effective protection of this fundamental right.

At the international level, the European regulatory model has become one of the principal benchmarks for the development of modern data protection systems. The legislative evolution initiated by Directive 95/46/EC and subsequently reinforced through the General Data Protection Regulation (GDPR) established a regulatory approach founded upon the principle of accountability, requiring organizations engaged in personal data processing to assume proactive responsibility for compliance. Rallo Lombarte (2019) argues that this new regulatory paradigm transformed data protection into a preventive legal framework in which risk management, transparency, and accountability became central pillars of digital governance.

The modernization of regulatory frameworks has likewise responded to the necessity of adapting traditional legal norms to emerging technological environments. Automated information processing, intelligent algorithmic systems, and the provision of digital services require regulatory frameworks that are sufficiently flexible to accommodate continuous technological innovation without undermining the effective protection of fundamental rights. In this regard, Penadés (2018) contends that the renewed European regulatory framework represents a structural transformation in the conception of data protection law by replacing predominantly formal compliance models with comprehensive systems focused on risk prevention and integrated governance.

Across Latin America, a gradual process of regulatory harmonization inspired by international standards is currently underway, although institutional development remains uneven among jurisdictions. Countries such as Colombia, Chile, Brazil, Mexico, and Ecuador have strengthened their legal frameworks by incorporating principles including lawfulness, informed consent, purpose limitation, data minimization, and controller accountability. Examining the regulation of electronic health records in Colombia, Contreras (2020) emphasizes that the digitalization of public services requires maintaining a continuous balance between efficient access to information and the preservation of the confidentiality of personal data, particularly when sensitive information is involved.

The implementation of these regulatory frameworks has also extended to public administrations and local governments, which manage extensive databases relating to healthcare, education, social security, taxation, and public services. The digital transformation

of the public sector necessitates strengthening institutional capacities to prevent violations of fundamental rights arising from large-scale information processing. In this respect, Asensio (2018) argues that public institutions should implement comprehensive compliance programs incorporating data protection impact assessments, internal information security policies, and continuous supervisory mechanisms, thereby fostering an organizational culture committed to the effective protection of personal data.

Processing of Personal Data

The processing of personal data encompasses the full range of operations performed on identifiable information, including its collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure, transfer, erasure, and any other form of automated or manual processing. Owing to the exponential growth of digital ecosystems, these activities have become integral and continuous functions within public institutions, private enterprises, and digital platforms, thereby increasing the need for robust legal obligations governing the management of personal information.

The initial stage of data processing involves the collection of personal data, which must be conducted in accordance with the principles of lawfulness, transparency, and informed consent. Subsequently, the storage of personal information requires the implementation of appropriate technical and organizational measures to ensure its confidentiality, availability, and integrity throughout the entire data lifecycle. Spain's former Organic Law 15/1999 on the Protection of Personal Data (Government of Spain, 1999) represented one of the earliest European legal instruments to establish specific obligations regarding secure data storage and restricted access to personal information, thereby laying important regulatory foundations for subsequent data protection legislation.

One of the most complex dimensions of contemporary data processing concerns international transfers of personal data. The globalization of digital services means that an individual's information may be stored, processed, or shared simultaneously across multiple jurisdictions, some of which do not provide an adequate level of legal protection. In response to this reality, Vergara Rojas (2017) argues that modern legislative initiatives seek to strengthen authorization mechanisms governing international data transfers by requiring safeguards equivalent to those established under the legal framework of the country of origin while reinforcing the supervisory powers of data protection authorities.

The evolution of legal scholarship has demonstrated that data processing should not be regarded merely as a technical operation but rather as a continuous legal responsibility. Consequently, entities determining the purposes and means of processing assume obligations relating to compliance management, risk assessment, cybersecurity governance, and the effective protection of data subject rights. From this perspective, Martínez (2007) maintains that personal data protection represents a concrete manifestation of the constitutional rule of law by imposing legal constraints on informational power and establishing effective mechanisms for individual oversight and accountability.

The strengthening of the accountability principle has generated new obligations for both data controllers and data processors, particularly where personal information is processed through automated technologies or artificial intelligence systems. Accountability, documentation of processing activities, notification of personal data breaches, and the adoption of preventive security measures have become fundamental requirements of contemporary digital law. García Hernández (2022) explains that the European regulatory framework substantially expanded civil liability arising from unlawful data processing by consolidating compensation mechanisms designed to ensure effective redress for damages suffered by data subjects.

Contemporary Challenges in Personal Data Protection

Digital transformation has generated significant benefits across the fields of economic development, education, healthcare, and public administration. Nevertheless, it has also intensified the risks associated with the large-scale processing of personal information. The emergence of technologies based on big data, artificial intelligence (AI), machine learning, and digital surveillance systems has dramatically expanded the capacity to collect, analyze, and exploit information relating to the daily activities of millions of individuals. Consequently, the protection of privacy now faces challenges that extend well beyond the capabilities of traditional regulatory models.

One of the principal challenges arises from the rapid expansion of big data analytics, understood as the processing of massive volumes of information originating from multiple digital sources. The ability to identify behavioral patterns, generate predictive insights, and construct highly detailed individual profiles significantly increases the risks of algorithmic discrimination, commercial manipulation, and the misuse of sensitive personal information. Pineda Castaño et al. (2020) argue that personal data protection should now be understood as an indispensable fundamental right for preserving human dignity within societies characterized by the continuous circulation of digital information.

Artificial intelligence constitutes another major challenge for contemporary legal systems due to the increasing deployment of automated systems capable of making decisions with significant legal, economic, and social consequences. The opacity of many algorithmic models complicates the effective exercise of rights such as access, rectification, and objection, thereby generating new tensions between technological innovation and the protection of fundamental rights. Within this context, Farfán Pinargote and Moreira Macías (2024) contend that the responsible development of artificial intelligence requires regulatory frameworks incorporating the principles of transparency, explainability, human oversight, and legal accountability in order to prevent potential violations of human rights.

The expansion of digital surveillance technologies likewise represents an increasingly significant challenge to the protection of privacy. The deployment of biometric identification systems, facial recognition technologies, continuous geolocation tracking, and automated monitoring mechanisms enables the permanent observation of individuals' activities in both physical and virtual environments. Although these technologies may contribute to public security and administrative efficiency, they also create substantial risks associated with mass surveillance and the erosion of individual freedoms. Díaz Méndez (2024) emphasizes that the effective protection of fundamental rights requires every technological surveillance measure to comply strictly with the principles of necessity, proportionality, and judicial oversight.

Finally, cybersecurity has become an indispensable pillar of personal data protection. The increasing frequency of cyberattacks, ransomware incidents, identity theft, and large-scale data breaches demonstrates that technological security constitutes a prerequisite for ensuring the effective realization of the rights guaranteed under data protection legislation. In this context, Morales-Sáenz et al. (2024) argue that digital security should be addressed through a multidimensional approach integrating public policy, digital literacy, international cooperation, and institutional capacity building. Consequently, the current state of the art demonstrates that effective personal data protection requires a comprehensive and multidisciplinary response in which legal regulation, technological innovation, digital governance, and a robust culture of respect for fundamental rights converge to address the complex challenges posed by the information society and the digital economy.

Discussion

The literature review revealed a broad scholarly consensus that the protection of personal data has evolved beyond being merely an extension of the right to privacy and has become an autonomous fundamental right within contemporary constitutional and international legal

frameworks. This evolution has been driven by the rapid expansion of digital technologies and the unprecedented capacity to collect, process, and exploit personal information on a massive and automated scale. In this regard, Conde Ortiz (2005) argues that the autonomy of this right lies in the individual's ability to exercise effective control over the processing of personal information. Expanding this perspective, Maqueo Ramírez et al. (2017) contend that the principal challenge for contemporary legal systems is to reconcile technological innovation with the effective protection of privacy and other fundamental rights within an increasingly interconnected global digital environment.

Another significant finding emerging from the analysis concerns the transformation of the traditional concept of privacy. Whereas early legal theories primarily sought to protect individuals against external intrusions into their private sphere, contemporary legal scholarship increasingly addresses the risks associated with algorithmic decision-making, artificial intelligence, and digital platforms. Along these lines, Talciani (1999) recognized privacy as an essential prerequisite for the free development of personality, a position that has subsequently been expanded by Castillo Parrilla (2023), who demonstrates that artificial intelligence may also affect collective rights through the creation of group profiles derived from the automated processing of large-scale datasets. This evolution reflects the transition from an individual-centered conception of privacy toward broader concerns regarding algorithmic governance and collective digital rights.

The review likewise identified substantial agreement among scholars regarding the fundamental role of the principles governing personal data processing. The principles of lawfulness, informed consent, purpose limitation, proportionality, and security consistently emerge as indispensable safeguards for ensuring the lawful and responsible processing of personal information. Pouillet and Dinant (2007) argue that these traditional principles require reinterpretation in response to increasingly complex digital environments, whereas Porcelli (2019) maintains that Ibero-American regulatory standards have progressively evolved toward governance models that reinforce transparency, accountability, and the responsibilities of entities processing personal data. Collectively, these perspectives demonstrate that the effectiveness of data protection regimes depends not only on the quality of legislative frameworks but also on their consistent implementation and institutional enforcement.

Regarding the rights of data subjects, the literature indicates that the formal recognition of the rights of access, rectification, erasure, objection, and data portability represents a significant advancement in the protection of informational self-determination. Nevertheless, important challenges remain in ensuring their effective exercise within increasingly complex technological environments. Bordachar Benoit (2022) identifies regulatory deficiencies in several Latin American legislative initiatives concerning the effective implementation of the ARCO rights, while Roldán Carrillo (2021) argues that the principles of consent and purpose limitation require more rigorous supervisory mechanisms in response to the growing use of artificial intelligence and automated decision-making systems. These findings suggest that strengthening digital rights requires not only comprehensive legal frameworks but also robust institutional capacities capable of guaranteeing their practical enforcement.

With respect to the regulatory framework, the review identified a clear trend toward the harmonization of national legal systems with international data protection standards, particularly those inspired by the European regulatory model. Rallo Lombarte (2019) emphasizes that the General Data Protection Regulation (GDPR) introduced a preventive governance model grounded in the principle of accountability, fundamentally transforming the regulatory philosophy of personal data protection. Similarly, Contreras (2020) demonstrates that the digitalization of sensitive public services, such as electronic health records, requires balancing technological innovation with strong legal safeguards to preserve confidentiality and fundamental rights. Consequently, the reviewed literature consistently indicates that

regulatory modernization constitutes an ongoing process shaped by the accelerating pace of technological innovation.

The processing of personal data also emerged as a central point of convergence within the analyzed literature. The collection, storage, dissemination, and international transfer of personal information impose increasingly complex obligations upon both data controllers and data processors. Within this context, Vergara Rojas (2017) warns that cross-border data transfers remain among the most significant regulatory challenges because of persistent disparities in the levels of legal protection provided by different jurisdictions. Complementing this perspective, García Hernández (2022) argues that the expansion of civil liability arising from unlawful data processing has strengthened the legal protection afforded to data subjects by incorporating more effective mechanisms for compensating damages resulting from the misuse of personal information. These contributions underscore the growing importance of accountability-based regulatory models within contemporary digital governance.

Finally, the review confirms that the most pressing contemporary challenges arise from the rapid development of big data analytics, artificial intelligence, digital surveillance technologies, and cybersecurity threats. Pineda Castaño et al. (2020) argue that these developments require personal data protection to be reconceptualized as an essential fundamental right within the digital society. Likewise, Farfán Pinargote and Moreira Macías (2024) emphasize the necessity of incorporating the principles of transparency, explainability, human oversight, and accountability into the regulation of artificial intelligence systems to mitigate potential risks to human rights. Furthermore, Morales-Sáenz et al. (2024) identify cybersecurity as an inseparable component of the legal protection of personal information, highlighting its strategic importance within contemporary digital governance. Taken together, these findings suggest that future regulatory frameworks must evolve toward more dynamic, interdisciplinary, and preventive governance models capable of responding effectively to technological innovation while preserving the effective exercise of fundamental rights and maintaining public trust in digital ecosystems.

Conclusions

The present review demonstrates that the protection of personal data constitutes an essential fundamental right for safeguarding privacy, informational self-determination, and human dignity within the digital society. The rapid evolution of information and communication technologies has significantly expanded the capacity to collect, store, and process personal information, generating substantial benefits across multiple sectors while simultaneously creating new risks to individual rights and freedoms. Consequently, legal and regulatory frameworks must evolve continuously to respond effectively to technological innovation and to maintain an appropriate balance between digital development, technological progress, and the effective protection of fundamental rights.

The findings further indicate that the principles of lawfulness, informed consent, purpose limitation, proportionality, and security remain the cornerstone of contemporary personal data protection regimes. These principles are complemented by the recognition of fundamental data subject rights, including the rights of access, rectification, erasure, objection, and data portability, which collectively reinforce individual control over personal information. Nevertheless, the effectiveness of these legal guarantees depends not only upon their formal recognition within legislative frameworks but also upon the existence of robust institutional structures, effective supervisory and enforcement mechanisms, and a well-established culture of regulatory compliance among organizations engaged in the processing of personal data within increasingly complex digital environments.

Finally, the review concludes that the most significant contemporary challenges arise from the rapid expansion of big data analytics, artificial intelligence, digital surveillance technologies,

and cybersecurity threats, all of which have substantially increased the complexity of personal data processing. Addressing these challenges requires strengthening regulatory frameworks, promoting international cooperation, and fostering a model of digital governance grounded in the principles of transparency, accountability, and respect for human rights. Through such an approach, it will be possible to consolidate resilient and adaptive personal data protection systems capable of responding effectively to the demands of technological transformation while preserving public trust in digital ecosystems and ensuring the long-term protection of fundamental rights.

Study Limitations

The principal limitation of this study lies in its documentary nature, as it was based exclusively on the analysis of scientific literature, legal instruments, and specialized legal scholarship without incorporating empirical evidence derived from field research or case studies that could have enabled the validation and contextualization of the findings.

Future Research

Future studies should prioritize empirical and comparative research evaluating the practical implementation and effectiveness of personal data protection legislation, as well as examining the legal and societal implications of artificial intelligence, big data, and other emerging technologies on the exercise and protection of digital rights across different legal systems.

Acknowledgments

The author expresses sincere gratitude to the scholars, researchers, and academics whose scientific, doctrinal, and methodological contributions made the development of this study possible. Special appreciation is extended to experts in digital law, personal data protection, and emerging technologies, whose research has enriched academic debate and advanced the understanding of the complex legal challenges arising from digital transformation. The author also gratefully acknowledges the valuable role of academic institutions and scientific publishers committed to promoting high-quality research and the dissemination of knowledge in the fields of fundamental rights and technology regulation.

Conflict of Interest Statement

The author declares, under their sole responsibility, that there are no personal, professional, academic, financial, or institutional conflicts of interest that could have influenced the design, conduct, analysis, interpretation, or publication of the findings presented in this study.

Referencias

- Anticona, W., Frias, J., Frias, R., & Ticona, I. (2023). Investigación cualitativa y mixta en derecho. tipología y la aplicación del metaanálisis cualitativo. *Revista de Climatología Edición Especial Ciencias Sociales*, 257.
- Arellano López, C. A. (2020). El derecho de protección de datos personales. *Biolex*, 12(23), 163-174.
- Asensio, R. J. (2018). El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales. *Anuario aragonés del gobierno local*, (10), 321-365.
- Avellaneda Vásquez, J. (2024). Metodología de investigación en Derecho y Literatura para la educación jurídica y derechos humanos. *Justicia*, 29(45). <https://doi.org/10.17081/just.29.45.7342>
- Bordachar Benoit, M. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO. *Revista chilena de derecho y tecnología*, 11(1), 397-414.

- Botero Bernal, A. (2016). Sobre el uso de la bibliografía en la investigación jurídica. *Pensamiento Jurídico*, (43).
- Cano, L. G. (2012). Protección de datos en Colombia, avances y retos. *Lebret*, (4), 195-214.
- Castillo Parrilla, J. A. (2023). Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial. *Derecho Privado y Constitución*, 43, 53-88.
- Conde Ortiz, C. (2005). La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad. Servicio de Publicaciones de la Universidad de Cádiz. URI: <http://hdl.handle.net/10498/26396>
- Contreras, A. F. (2020). Marco normativo de la historia clínica electrónica y su incidencia en el ámbito de la protección de datos personales en Colombia. *Revista la propiedad inmaterial*, 29, 95.
- Cordero Alemán, S. R. (2023). Protección jurídica, habeas data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales. [Tesis de grado, Universidad de Cuenca]. <http://dspace.ucuenca.edu.ec/handle/123456789/43392>
- de España, G. (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Bol Del Estado*, 298(2), 43088-43099.
- Díaz Méndez, E. M. (2024). Desafíos contemporáneos en la protección del derecho a la libertad personal frente a medidas de seguridad. *Revista Diversidad Científica*, 4(2), 193-203.
- Drummond, V. (2004). Internet, privacidad y datos personales. Editorial Reus.
- Farfán Pinargote, D. F., & Moreira Macías, K. A. (2024). Protección de datos personales: desafíos y garantías en la era digital y los derechos humanos.
- García Hernández, A. (2022). Responsabilidad civil de encargados y responsables del tratamiento de datos en el Reglamento UE de Protección de Datos. *Revista CESCO de Derecho de Consumo*, (41), 132-158.
- García, M. P. (2019). Impacto de las tecnologías digitales en la transformación del comercio internacional. *Cuadernos de Información económica*, 268, 65-76.
- Giménez, A. O., Real, D. M. D., & García, D. M. E. M. (2015). La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita. *Madrid: Agencia Española de Protección de Datos*, 61.
- González Guerrero, L. D. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, 21(1), 209-244.
- López-Torres, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. *Ejil-EAFIT Journal of International Law*, 5(2), 103-117.
- Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, 30(1), 77-96.
- Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: una amenaza para los datos personales. *Rev. Prop. Inmaterial*, 27, 5.
- Martínez, R. M. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, (5), 4.
- Morales-Sáenz, F. I., Medina-Quintero, J. M., & Rodríguez, F. O. (2024). Seguridad digital y violencias estructurales: perspectivas y desafíos contemporáneos. *Dilemas*

- Contemporáneos: Educación, Política y Valores.* DOI: <https://doi.org/10.46377/dilemas.v12i.4486>
- Parra Domínguez, M. L., & Briceño Rodríguez, I. I. (2013). Aspectos éticos en la investigación cualitativa. *Revista De Enfermería Neurológica*, 12(3), 118-121. <https://doi.org/10.51422/ren.v12i3.167>
- Penadés, J. P. (2018). El nuevo marco normativo de la protección de datos. *Actualidad civil*, 5.
- Pineda Castaño, L. M., Mondragón Duarte, S. L., & Moreno Mosquera, V. J. (2020). Protección de datos como derecho fundamental en la sociedad global: una mirada desde los desafíos contemporáneos de la pospandemia. Visión integral de la pospandemia desde la perspectiva socioeconómica en el contexto global, 16-24. Alianza de Investigadores Internacionales S.A.S Alinin
- Porcelli, A. M. (2019). La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos. *Revista Quaestio Iuris*, 12(2), 465-497.
- Poullet, Y., & Dinant, J. M. (2007). Hacia nuevos principios de protección de datos en un nuevo entorno TIC. *IDP. Revista de Internet, Derecho y Política*, (5), 33-46.
- Rallo Lombarte, A. (2019). EL NUEVO DERECHO DE PROTECCIÓN DE DATOS. *Revista española de derecho constitucional*, (116).
- Rivera Barrantes, V. (2019). Realidad sobre la privacidad de los datos personales en Costa Rica. *E-Ciencias de la Información*, 9(2), 68-81.
- Rojas-Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus: Revista Especializada en Sociología Jurídica y Política*, 8(1), 107-139. doi:<http://dx.doi.org/10.14718/NovumJus.2014.8.1.6>
- Roldan Carrillo, F. N. (2021). Los ejes centrales de la protección de datos: Consentimiento y finalidad: Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review*, 8(1), 175-202.
- Talciani, H. C. (1999). Vida familiar y derecho a la privacidad. *Revista Chilena de Derecho*, 26, 63.
- Vergara Rojas, M. (2017). Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. *Revista chilena de derecho y tecnología*, 6(2), 135-152.
- Zambrano Mera, I. E., & Chancay García, L. (2024). Impacto de las tecnologías digitales en el aprendizaje y la enseñanza en entornos educativos. *Qualitas Revista Científica*, 28(28), 054 - 068. <https://doi.org/10.55867/qual28.04>