J. Law Epistemic Stud. (July - December 2024) 2(2): 7-12
https://doi.org/10.5281/zenodo.15252711

JLES
JOURNAL OF LAW AND EPISTEMIC STUDIES

ORIGINAL ARTICLE

Data protection and privacy in the context of emerging technologies

Protección de datos y privacidad en el contexto de las tecnologías emergentes

Angélica M. Hernández

Received: 03 April 2024 / Accepted: 01 May 2024 / Published online: 07 July 2024

Abstract This study analyzed the challenges faced by traditional personal data protection mechanisms in the face of the advances of emerging technologies such as artificial intelligence, the Internet of Things, and neurotechnology. The objective was to examine the relationship between regulatory awareness, risk perception, and institutional practices related to data processing. To this end, a quantitative methodology was applied through a structured survey with a stratified sample of digital technology users. The data were analyzed using descriptive and inferential statistical techniques. The results showed a direct correlation between regulatory awareness and perceptions of digital security and a critical outlook among users with greater technological exposure. A gap was also identified between declared institutional policies and their actual implementation. The analysis allowed for the segmentation of user profiles and highlighted the need for more effective consent mechanisms, algorithmic auditing, and digital education. The conclusion was that adopting a comprehensive approach that articulates technological innovation, dynamic regulation, and citizen empowerment is essential to build digital governance based on protecting fundamental rights.

Keywords personal data protection, digital privacy, emerging technologies, informed consent, artificial intelligence, neurotechnology.

Resumen El presente estudio analizó los desafíos que enfrentan los mecanismos tradicionales de protección de datos personales ante el avance de tecnologías emergentes como la inteligencia artificial, el internet de las cosas y la neurotecnología. Se planteó como objetivo examinar la relación entre el nivel de conocimiento normativo, la percepción de riesgo y las prácticas institucionales vinculadas al tratamiento de datos. Para ello, se aplicó una metodología cuantitativa mediante una encuesta estructurada, con una muestra estratificada de usuarios de tecnologías digitales. Los datos fueron analizados mediante técnicas estadísticas descriptivas e inferenciales. Los resultados evidenciaron una correlación directa entre el conocimiento normativo y la percepción de seguridad digital, así como una visión crítica por parte de los usuarios con mayor exposición tecnológica. También se identificó una brecha entre las políticas institucionales declaradas y su implementación real. El análisis permitió segmentar perfiles de usuarios y subrayó la necesidad de mecanismos más efectivos de consentimiento, auditoría algorítmica y educación digital. Se concluyó que es imprescindible adoptar un enfoque integral que articule innovación tecnológica, regulación dinámica y empoderamiento ciudadano, con el fin de construir una gobernanza digital basada en la protección de los derechos fundamentales.

Palabras clave protección de datos personales, privacidad digital, tecnologías emergentes, consentimiento informado, inteligencia artificial, neurotecnología.

How to cite
Hernández, A. M. (2024). Data protection and privacy in the context of emerging technologies. *Journal of Law and Epistemic Studies*, *2*(2), 7-12. https://doi.org/10.5281/zenodo.14868646

Angélica M. Hernández
a.hdezp009@gmail.com

Universidad de Sancti Spíritus "José Martí Pérez", Cuba.

PUBLIS EDITORIAL

Introduction

Mass digitalization and the proliferation of emerging technologies have reshaped traditional notions of privacy and data protection. Today, connected devices, artificial intelligence (AI) systems, neurotechnology, and ubiquitous computing environments collect, process, and interpret personal data in an automated and persistent manner (Magee et al., 2024).

This transformation has increased the strategic value of personal data and multiplied the risks of rights violations, particularly when consent mechanisms are opaque or technological architectures do not comply with traditional legal frameworks (Zhu et al., 2023; Pinto et al., 2024). For example, centralized digital environments such as social networks, digital health services, and even educational platforms collect large volumes of data without users having absolute control over the destination of their information, resulting in what some authors call "informational asymmetry" (Ehimuan et al., 2024).

In this context, the rise of neurocognitive technologies, such as brain-computer interfaces (BCIs), which allow mental states to be inferred from neural signals, stands out, generating unprecedented challenges around neuroprivacy. Recent studies show that users are interested in these technologies and are growing concerned about privacy and the lack of transparency in using their neuro data (Kablo & Arias-Cabarcos, 2023). As Magee et al. (2024) argue, developing devices capable of capturing cognitive biometrics introduces new risks beyond traditional data protection frameworks, demanding specific regulatory reforms.

At the same time, the emergence of generative AI tools, blockchain, big data, and immersive technologies raises key questions about the actual capacity of current legal frameworks to provide adequate safeguards. According to García et al. (2024), blockchain technology's decentralization, traceability, and immutability can significantly contribute to consent and digital identity management. However, they also present limitations when not combined with advanced privacy mechanisms such as homomorphic encryption or off-chain storage. Immersive technologies such as the metaverse also present specific privacy risks that have been widely studied (Wang et al., 2022).

On the other hand, there is growing concern about the processing of personal data in IoT ecosystems. Pinto et al. (2024) conducted a systematic review of privacy solutions in personal data stores, concluding that while these technologies can return control to the user, their practical adoption remains limited and requires clear regulatory frameworks that promote their implementation, especially in cloud architectures combined with artificial intelligence (Dhinakaran et al., 2024). Similarly, Ehimuan et al. (2024) warn that the exponential growth in technologies such as artificial intelligence and big data analytics has exceeded the response capacity of many regulatory frameworks, opening the door to systemic and cross-border privacy breaches.

Furthermore, advancing technologies such as self-sovereign digital identities and blockchain-based consent management mechanisms have sparked interest in contemporary literature as complementary tools to strengthen individual control over personal data (García et al., 2024). These proposals point to a new regulatory logic that goes beyond centralized models, incorporating principles of informational self-determination, traceability, and algorithmic transparency.

In short, protecting personal data in emerging technological contexts requires a profound rethinking of existing regulatory and technological strategies. This article proposes an empirical and normative approach that combines statistical analysis of citizen perception with a critical review of the state of the art to propose guidelines for ethical, inclusive, and rights-centered digital governance. The urgency of this debate is even more evident given the institutional inertia and regulatory gaps that allow data collection, processing, and exploitation practices without due process or effective oversight by the data subjects. This regulatory gap is especially worrying in regions such as Latin America, where regulatory evolution is moving more slowly (Mendoza & Enríquez, 2024).

In this scenario, integrating ethical principles into the design of technologies becomes imperative. The concept of "privacy by design," reflected in regulations such as the GDPR and promoted by institutions such as the Spanish Data Protection Agency (AEPD, 2024), implies that technological developments must incorporate mechanisms for privacy protection, data minimization, and transparency in the processing of personal information from their initial stages (Ehimuan et al., 2024). This proactive perspective is key to overcoming reactive approaches based solely on post-infringement sanctions.

Likewise, consent's role as a data protection pillar must be rethought. Various studies indicate that, in contexts dominated by algorithms and automation, informed consent loses effectiveness if users do not understand the future uses of their data or if it is transferred to third parties through opaque contractual clauses (Kablo & Arias-Cabarcos, 2023; Pinto et al., 2024).

Therefore, dynamic consent systems, with revocation options and granular control, are needed and tailored to the evolving logic of digital environments. Furthermore, recent studies have warned that the indiscriminate use of AI-based technologies can generate adverse psychological impacts, especially in minors (Mansfield, 2025).

Likewise, the data protection challenges in emerging technologies cannot be separated from digital education. Privacy literacy must be a priority for citizens and professionals in the public and private sectors, given that understanding rights and responsibilities is a determining factor in effectively exercising digital autonomy. This training must include technical, legal, and ethical dimensions adapted to different educational levels and sociocultural contexts.

Finally, international cooperation is consolidated as essential for addressing global privacy challenges in the digital age. Regulatory gaps between regions encourage data forum shopping and limit the sanctioning power of local authorities. Therefore, creating minimum international standards and mutual legal assistance mechanisms is crucial for building an interoperable digital ecosystem that respects human rights (Ehimuan et al., 2024; García et al., 2024).

Contemporary literature agrees that emerging technologies have displaced traditional models of personal data processing, generating unprecedented challenges around neuro privacy (Xia et al., 2024). The European Union's General Data Protection Regulation (GDPR) has established fundamental principles such as data minimization, portability, and explicit consent, becoming the global benchmark for privacy regulatory frameworks. However, recent studies warn that this framework is insufficient in the face of new risks arising from artificial intelligence, machine learning, and biometric recognition systems (Ehimuan et al., 2024).

From a more specific perspective, recent research identifies three significant gaps in current legislation: the lack of international harmonization, the weakness of oversight bodies, and citizens' low digital literacy (Rachut & Maurer, 2024). These limitations hinder the effective exercise of rights such as access, rectification, or opposition to data processing, especially when collected in cross-border contexts or through opaque technologies.

At the technical level, several investigations propose using decentralized technologies such as blockchain and anonymization techniques powered by artificial intelligence (Yang et al., 2024) to strengthen consent, traceability, and access control mechanisms. Zhu et al. (2023) propose a model based on smart contracts and distributed encryption that would allow users to negotiate access to their data under economic compensation schemes, automated auditing, and data altruism models such as those proposed in the European context (Rachut & Maurer, 2024).

Similarly, García et al. (2024) explore the potential of self-sovereign digital identities (SSIs) as tools to give people back control over their informational identity.

The literature warns that current regulations lack specific protection mechanisms regarding highly sensitive technologies, such as neurotechnology. Kablo and Arias-Cabarcos (2023) show, based on an empirical study with users of brain-computer interfaces, that there is a high level of acceptance of these technologies but also a low awareness of the risks they pose to mental freedom, cognitive autonomy, and emotional privacy. This has led some countries, such as Chile, to recognize neuro-rights in their constitutional legislation in an attempt to anticipate the commercial exploitation of brain data.

In short, the review of the state of the art highlights the urgent need to move toward a new regulatory and technological model that considers the dynamic, ubiquitous, and predictive nature of data processing in the context of emerging technologies. The literature supports a comprehensive strategy that combines adaptive regulation, responsible innovation, protection by design, and citizen empowerment.

A relevant aspect addressed by Pinto et al. (2024) in their systematic review of privacy in the context of the Internet of Things (IoT) is the low adoption of personal data stores (PDS), which would allow users to store, manage, and authorize access to their information from a decentralized perspective. Despite their potential, only 20% of the studies reviewed propose practical solutions based on this approach, revealing a gap between theoretical developments and their actual application in mass-use environments.

For their part, Zhu et al. (2023) show how the centralized architecture of traditional web services places users in a position of weakness vis-à-vis service providers. The authors argue that users are forced to provide personal data in exchange for access to platforms without a clear understanding of how this information will be used later, giving rise to a phenomenon known as a "forced privacy trade-off."

The study by García et al. (2024) also emphasizes that while blockchain promises decentralization and traceability, it does not guarantee privacy protection. End-to-end encryption, off-chain storage, and autonomous consent management are essential for achieving an effective privacy architecture, especially in multi-stakeholder, multi-sector environments.

Furthermore, recent research by Pinto et al. (2024) highlights the importance of categorizing IoT privacy risks into dimensions such as tracking, identification, profiling, and inventory attacks. This classification allows for better visualization of users' challenges when their information circulates between interconnected devices. It raises the need for protection standards tailored to the granularity and context of the collected data.

Another critical dimension highlighted by García et al. (2024) is interoperability across platforms and jurisdictions. In a globalized world, where data may be generated in one country, processed in another, and stored in a third, coordinated and compatible legal systems are required. The authors emphasize that adopting open identity and consent standards would resolve regulatory conflicts and ensure respect for digital rights across national borders.

For their part, the study by Zhu et al. (2023) documents through Stackelberg game simulations that it is possible to model economic incentives for companies to actively participate in protecting their users' data. By distributing revenues from data trading between users and providers, the model demonstrates how it is feasible to align market interests with ethical privacy principles within a technical and contractual governance framework.

Finally, Ehimuan et al. (2024) emphasize that any practical approach to data protection must consider the social and cultural context. Perceptions of privacy vary across populations, so they propose a multilevel approach that combines standard regulations with contextual adaptations and privacy education policies. Only in this way, they argue, can we move toward an inclusive, fair, and sustainable digital ecosystem.

Regarding digital governance, Ehimuan et al. (2024) highlight the importance of adopting dynamic regulatory frameworks that evolve with technology. They propose a comprehensive, coherent, and inclusive regulatory approach that harmonizes data protection principles and incorporates effective oversight mechanisms, proportional sanctions, and redress systems for those affected by privacy violations. This approach seeks to bridge the gap between innovation and legal accountability in an environment of rapid digital transformation.

Methodology

This study adopted a quantitative, non-experimental, cross-sectional, correlational methodological approach. The objective was to examine the relationship between user perceptions of data protection and the use of emerging technologies such as artificial intelligence, IoT, blockchain, and neurotechnology.

Population and Sample: The target population was digital service users, academics, and professionals from Latin America's technology and legal sectors. Stratified sampling by sector (public, private, academic) was used, with an estimated minimum sample size of 150 participants.

Instrument: A structured online questionnaire was administered, consisting of 20 items organized on 5-point Likert-type scales. The instrument was divided into four dimensions: level of regulatory knowledge in data protection, risk perception and technological confidence, frequency of use of emerging technologies, and opinion on consent mechanisms and algorithmic transparency.

Procedure: The questionnaire was distributed through digital platforms, institutional emails, and professional networks. Following the ethical principles of social research, participants' anonymity and informed consent were guaranteed.

Data collection took place between November and December 2024. Participation was voluntary, and users residing in Latin American countries, primarily Ecuador, Colombia, Mexico, and Peru, were targeted, allowing for various institutional and regulatory contexts.

Analysis techniques: Data were processed using statistical software (SPSS or R). Descriptive analyses (mean, standard deviation, frequencies), hypothesis tests (chi-square, Student's t-test, ANOVA), and multivariate models (logistic regression and exploratory factor analysis) were used to identify significant associations between variables.

This methodology allowed us to identify patterns of perception and behavior and statistically validate hypotheses about the impact of emerging technologies on personal privacy from an empirical and comparative perspective.

Results and discussion

The results obtained from the survey analysis revealed a positive correlation between the level of normative/legal knowledge and the perception of digital security. Specifically, participants with greater familiarity with frameworks such as the GDPR or the CCPA tended to adopt a more critical stance toward using emerging technologies, demanding stronger safeguards in consent mechanisms, access to information, and algorithmic transparency.

Table 1 presents a typology of user profiles based on their level of regulatory knowledge, frequency of emerging technology use, risk perception, and trust in current legal mechanisms. This classification helps identify key patterns in the interaction between legal awareness, technology adoption, and data protection concerns, highlighting how these variables relate across different user groups. The results reveal significant divergences, particularly regarding distrust of legal systems among highly informed users, compared to greater acceptance among those with less technical-regulatory knowledge.

Likewise, users with frequent experience using artificial intelligence, Internet of Things (IoT) devices, and platforms employing biometric authentication expressed greater skepticism regarding the effectiveness of current personal data protection strategies. This perception reinforces the findings of Pinto et al. (2024) and García et al. (2024), who argue that direct exposure to sensitive technologies tends to intensify privacy concerns.

Within institutional settings, the data revealed a significant gap between reported regulatory compliance and the internal perception of its enforcement. Although most respondents indicated that their organizations had data protection policies, fewer than 40% believed they were effectively and con-

Table 1. Classification of user profiles by digital literacy, technology use, and privacy concerns

User profile	Level of normative/ Legal knowledge	Frequency of emerging technology use	Perceived risk	Trust in existing legal mechanisms
Critical and highly informed	High	High	High	Low
Technologically active, moderate	Medium	High	Medium	Medium
Low knowledge, limited interaction	Low	Low	Low	Relatively high

sistently implemented.

The multivariate analysis identified three main user clusters: a highly informed and critical group, a moderately informed but technologically active group, and a third group characterized by low levels of legal knowledge and limited digital interaction. These findings are consistent with the literature advocating for differentiated approaches to regulatory and educational interventions (Ehimuan et al., 2024).

From an interpretative standpoint, the results support the need for data protection models that integrate technological solutions with strong digital literacy and more effective institutional oversight mechanisms. The perceptions gathered indicate that, although a broadly recognized legal framework exists, its effectiveness largely depends on the degree of civic engagement and the genuine commitment of entities responsible for data processing.

These findings also align with the arguments made by Magee et al. (2024), who contend that the advancement of cognitive biometric technologies compels a rethinking of current legal frameworks through an approach that safeguards mental privacy. The high level of user distrust toward automated monitoring systems suggests that consent principles must evolve into more granular, informed, and revocable models, as also proposed by Kablo and Arias-Cabarcos (2023) in the context of neurotechnology.

Similarly, the results are consistent with Zhu et al. (2023) findings regarding the need for frameworks that allow users to actively negotiate the use of their data. This perspective contrasts with the current model of passive consent and reinforces the proposal to implement blockchain-based architectures to enable traceability, access management, and algorithmic auditing.

From a governance perspective, the empirical findings reinforce the thesis advanced by Ehimuan et al. (2024) concerning the urgent need to adopt global, dynamic, and culturally contextualized regulatory frameworks. The widespread perception among users of institutional opacity and limited regulatory effectiveness underscores the need to harmonize regulatory principles with interoperable technologies—an approach also advocated by Garcia et al. (2024), who propose self-sovereign digital identities as a mechanism for citizen empowerment.

Taken together, the data analyzed support the argument that current data protection mechanisms must undergo a comprehensive transformation, incorporating active user participation, privacy by design, and algorithmic transparency as foundational pillars of a new digital trust architecture.

Conclusions

The study reveals that existing personal data protection frameworks remain inadequate for addressing challenges posed by emerging technologies, with inconsistent implementation of regulations like the GDPR, especially in cross-border and technologically advanced scenarios. Findings indicate that normative awareness directly shapes risk perception, underscoring the importance of combining legislative reforms with robust public education initiatives. Current consent mechanisms prove insufficient, demanding a shift toward dynamic, user-centric models. A significant gap exists between institutional privacy policies and their practical application, highlighting the need for stronger governance, transparency measures, and systematic technical audits. Data protection must be embedded in technology design from inception, transforming principles like privacy by design, granular consent, and algorithmic transparency from theoretical concepts into enforceable standards. Achieving ethical and sustainable digital governance ultimately requires a threefold alignment: an empowered citizenry, responsible technological innovation, and adaptive regulatory frameworks capable of evolving with the digital landscape.

References

AEPD. (2024). *Innovación y Tecnología*. Agencia Española de Protección de Datos. https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia

Dhinakaran, D., Udhaya Sankar, S. M., Selvaraj, D., & Edwin Raja, S. (2024). Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration. *arXiv preprint*. https://arxiv.org/abs/2401.00794

Ehimuan, B., Chimezie, O., Akagha, O. V., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws:

A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews, 21*(2), 1058-1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

García, R. D., Ramachandran, G., Dunnett, K., Jurdak, R., Ranieri, C., Krishnamachari, B., & Ueyama, J. (2024). A survey of blockchain-based privacy applications: An analysis of consent management and self-sovereign identity approaches. *ACM*. https://arxiv.org/abs/2411.16404

Kablo, E., & Arias-Cabarcos, P. (2023). Privacidad en la era de la neurotecnología. In *Proceedings of the 2023 ACM SIGSAC Conference*. https://doi.org/10.1145/3576915.3623164

Magee, P., Ienca, M., & Farahany, N. (2024). Beyond neural data: Cognitive biometrics and mental privacy. *Neuron, 112*. https://doi.org/10.1016/j.neuron.2024.09.004

Mansfield, K. L. (2025). Un estudio señala los peligros que supone la IA para la salud mental de niños y adolescentes. *The Lancet*. https://elpais.com/ciencia/2025-01-21/un-estudio-senala-los-peligros-que-supone-la-ia-para-la-salud-mental-de-ninos-y-adolescentes.html

Mendoza, A., & Enríquez, L. (2024). *Desafíos del derecho a la protección de datos personales en la era digital*. Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. https://www.infocdmx.org.mx/images/biblioteca/2024/DesafiosDerecho-PDP_EraDigital.pdf

Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A systematic review on privacy-aware IoT personal data stores. *Sensors, 24*(2197). https://doi.org/10.3390/s24072197

Rachut, S., & Maurer, J. W. (2024). Altruismo de datos en el marco del Reglamento Europeo de Gobernanza de Datos, ¿un acierto o mejorable? *Revista de Derecho Comunitario Europeo, 78*, 183-213. https://recyt.fecyt.es/index.php/RDCE/article/view/107334/79601

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *arXiv preprint*. https://arxiv.org/abs/2203.02662

Xia, K., Duch, W., Sun, Y., Xu, K., Fang, W., Luo, H., Zhang, Y., Sang, D., Xu, X., Wang, F-Y., & Wu, D. (2024). Privacy-preserving brain-computer interfaces: A systematic review. *arXiv preprint*. https://arxiv.org/abs/2412.11394

Yang, L., Tian, M., Xin, D., Cheng, Q., & Zheng, J. (2024). AI-driven anonymization: Protecting personal data privacy while leveraging machine learning. *arXiv preprint*. https://arxiv.org/abs/2402.17191

Zhu, R., Wang, M., Zhang, X., & Peng, X. (2023). Investigation of personal data protection mechanism based on blockchain technology. *Scientific Reports, 13*, 21918. https://doi.org/10.1038/s41598-023-48661-w

Conflicts of interest

The author declares that have no conflicts of interest.

Author contributions

Angélica M. Hernández: Conceptualization, data curation, formal analysis, investigation, methodology, supervision, validation, visualization, drafting the original manuscript and writing, review, and editing.

Data availability statement

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Statement on the use of AI

The author acknowledges the use of generative AI and AI-assisted technologies to improve the readability and clarity of the article.

Disclaimer/Editor's note

The statements, opinions, and data contained in all publications are solely those of the individual authors and contributors and not of Journal of Law and Epistemic Studies.

Journal of Law and Epistemic Studies and/or the editors disclaim any responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products mentioned in the content.