



Protección de datos personales en era digital

Personal data protection in the digital age

Daysi Alexandra Tayupanta-Guangatal
daysitg47@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua, Ecuador
<https://orcid.org/0009-0000-1220-7082>

María Cristina Mafla-Sánchez
mariams22@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua, Ecuador
<https://orcid.org/0009-0002-2940-6007>

Naomy Hurtado-Acosta
naomiha71@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua, Ecuador
<https://orcid.org/0009-0007-8073-4897>

Iruma Alfonso-González
ua.irumaalfonzo@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua, Ecuador
<https://orcid.org/0000-0001-6866-4944>

RESUMEN

El presente artículo ofrece una revisión bibliográfica sobre la Protección de datos personales en era digital procurando su aplicación en el contexto jurídico ecuatoriano. Mediante un análisis jurídico-documental de 15 documentos académicos, Los resultados revelan vacíos regulatorios en materia de consentimiento para tratamientos masivos, transferencia internacional de datos, seguridad en infraestructuras de computación en la nube y transparencia algorítmica. Se propone fortalecer las capacidades de supervisión institucional, adoptar enfoques privacy-by-design, promover la alfabetización digital ciudadana y armonizar la normativa interna con estándares internacionales como el RGPD y el Convenio 108+. Tales lineamientos resultan esenciales para garantizar un desarrollo digital inclusivo y respetuoso de los derechos fundamentales.

Descriptores: gobernanza de internet; derecho del ciberespacio; legislación de las comunicaciones. (Fuente: Tesauro UNESCO).

ABSTRACT

This article offers a literature review on personal data protection in the digital age, seeking its application in the Ecuadorian legal context. Through a legal-documentary analysis of 15 academic documents, the results reveal regulatory gaps in the areas of consent for mass processing, international data transfer, security in cloud computing infrastructures, and algorithmic transparency. It proposes strengthening institutional oversight capacities, adopting privacy-by-design approaches, promoting digital literacy among citizens, and harmonising internal regulations with international standards such as the GDPR and Convention 108+. Such guidelines are essential to ensure inclusive digital development that respects fundamental rights.

Descriptors: internet governance; cyberspace law; communication legislation. (Source: UNESCO Thesaurus).

Recibido: 13/10/2024. Revisado: 23/10/2024. Aprobado: 03/11/2024. Publicado: 21/11/2024.

Sección artículos de investigación



INTRODUCCIÓN

La acelerada digitalización de la sociedad ecuatoriana ha reconfigurado la esfera privada y plantea desafíos inéditos para el Estado constitucional de derechos y justicia. En el denominado *espacio de los flujos*, caracterizado por la circulación transfronteriza de información que describe Castells (2020), la protección de los datos personales emerge como un eje cardinal de la autodeterminación informativa y de la tutela del derecho a la intimidad, reconocido en los artículos 66.19 y 92 de la Constitución. No obstante, la creciente interconexión de dispositivos y servicios sitúa a los ciudadanos ante “riesgos sistémicos” que, según Romansky (2022), superan el paradigma clásico de confidencialidad y exigen respuestas normativas y técnicas integrales.

Estos riesgos se amplifican en sectores estratégicos. El auge de la *fintech* impulsado por políticas de inclusión financiera, presupone el tratamiento masivo de datos sensibles, lo que obliga a articular el principio de proporcionalidad con la preservación de la estabilidad del sistema de pagos, tal como advierten Gabor y Brooks (2020). Asimismo, las lecciones derivadas de la pandemia evidenciaron que la recopilación de datos sanitarios puede tensionar el límite entre el interés público y el respeto a la privacidad; de ahí que Ienca & Vayena (2020) destaquen la necesidad de salvaguardias rigurosas cuando se justifique el uso de información biomédica para fines de salud pública. A su vez, la progresiva migración hacia infraestructuras de cómputo en la nube exige como señalan Yang et al. (2020), un marco fortalecido de seguridad y de gobernanza que garantice la localización, integridad y disponibilidad de la información frente a proveedores *off-shore*.

En este contexto, el presente artículo ofrece una revisión bibliográfica sobre la Protección de datos personales en era digital procurando su aplicación en el contexto jurídico ecuatoriano.



MÉTODO

El artículo se desarrolló mediante un análisis jurídico-documental de alcance cualitativo y exploratorio, sustentado en la revisión crítica y sistemática de fuentes normativas, jurisprudenciales y doctrinales relevantes para la protección de datos personales en el Ecuador. Primero, se recopiló el corpus legislativo como Constitución de 2008, Ley Orgánica de Protección de Datos Personales y reglamentos conexo, junto con sentencias de la Corte Constitucional y del Tribunal de Justicia de la Comunidad Andina emitidas entre 2010 y 2024.

En paralelo se efectuó una búsqueda en bases indexadas (Scopus, Web of Science y RedALyC) y repositorios oficiales, utilizando descriptores como *protección de datos*, *privacidad digital* y *economía de plataformas*, filtrando únicamente textos académicos publicados en los últimos cinco años, procesándose una población de 15 artículos científicos para ser procesados en concordancia de construir la sección de resultados.

RESULTADOS

La acelerada transformación digital que atraviesan los sectores productivos en Ecuador reconfigura la noción misma de privacidad y exige revisar el alcance de la Ley Orgánica de Protección de Datos Personales (LOPDP, Registro Oficial N.º 459-S, 26-V-2021). En efecto, el paradigma de la *educación 4.0* descrito por Bonfield et al. (2020) demuestra que el tratamiento masivo de datos estudiantiles es consustancial a las nuevas metodologías de aprendizaje; sin embargo, dicha intensificación tecnológica entraña riesgos de perfilamiento y decisiones automatizadas que la LOPDP intenta mitigar mediante los principios de licitud, finalidad y minimización. De forma análoga, la “*space of flows*” de Castells (2020) evidencia que el carácter ubicuo de la información diluye fronteras territoriales, de modo que la autoridad ecuatoriana de control deberá robustecer los mecanismos de transferencia internacional de datos para garantizar un nivel adecuado de protección conforme al artículo 44 de la LOPDP.



En el ámbito económico, la digitalización financiera analizada por Gabor & Brooks (2020) en el contexto *fintech* plantea un doble desafío: ampliar la inclusión sin menoscabar la seguridad de los datos sensibles. Para el caso ecuatoriano, donde los servicios de banca móvil se expanden en zonas rurales, la exigencia de consentimiento expreso cobra una dimensión particular, toda vez que el marco constitucional (art. 92) reconoce el *habeas data* como acción expedita de control. A propósito de la pandemia, Ienca & Vayena (2020) y Keesara et al. (2020) muestran cómo la recopilación masiva de información sanitaria se justificó por razones de salud pública; no obstante, tales precedentes evidencian la necesidad de que el legislador ecuatoriano delimite claramente los supuestos de interés público y emergencia que habilitan el tratamiento de datos sensibles de salud, tal como exige el artículo 28 de la LOPDP.

Por su parte, los estudios de marketing digital (Kumar et al., 2021; Lee & Lee, 2020; Libai et al., 2020) ponen de relieve la capacidad de las plataformas para generar perfiles de consumidor mediante algoritmos de IA. Bajo la óptica ecuatoriana, la obligación de transparencia algorítmica y la tutela del derecho a la no discriminación automatizada reconocida expresamente en los artículos 50 y 51 de la LOPDP adquiere relevancia ante prácticas de publicidad segmentada agresiva, donde la línea entre personalización y vulneración de la autodeterminación informativa resulta difusa. En igual sentido, Parker & Grote (2022) destacan que el rediseño del trabajo mediado por algoritmos incrementa la asimetría de poder entre empleador y trabajador, lo que impone revisar la normativa laboral ecuatoriana para reconocer el derecho a la explicación de las decisiones automatizadas que afecten la continuidad o el desempeño laborales.

La industria turística, analizada por Pencarelli (2020), ilustra cómo la hiperpersonalización del servicio depende de la recolección constante de datos geolocalizados. Dado que Ecuador promueve la reactivación turística post-pandémica a través de plataformas digitales, el principio de minimización resulta esencial para impedir la sobreexposición de la huella de movilidad del usuario. Asimismo, la proliferación de *influencers*—fenómeno descrito por Rachmad (2024)



agrava la vigilancia comercial, pues su modelo de negocio se cimenta en el intercambio de datos sobre preferencias y comportamiento, esto exige que la Superintendencia de Protección de Datos Personales vigile la trazabilidad del consentimiento en campañas de mercadotecnia de afiliados.

En el plano técnico-jurídico, Romansky (2022) y Romansky & Noninska (2020) advierten que la convergencia entre big data e internet de las cosas multiplica las oportunidades de ataque a la confidencialidad, integridad y disponibilidad de la información. Ecuador, como Estado andino, todavía carece de reglamentos infralegales que detallen estándares de cifrado, anonimización y auditoría de riesgos. A este respecto, las tendencias identificadas por Yanamala & Suryadevara (2023), uso de inteligencia artificial para detección de brechas y respuesta a incidentes, sugieren la necesidad de políticas públicas que incentiven la adopción de *privacy-by-design* y la certificación de cumplimiento normativo (*compliance*) en organizaciones públicas y privadas.

En cuanto a la encuesta realizada por Yang et al. (2020) sobre seguridad y privacidad en la nube subraya la dependencia creciente de infraestructuras *off-shore*. Dicha realidad resalta la urgencia de suscribir acuerdos de adecuación con jurisdicciones terceras y de fomentar *data centers* locales que operen bajo estándares ISO/IEC 27701. En suma, la LOPDP constituye un avance significativo, pero su eficacia dependerá de la capacidad institucional para fiscalizar sectores estratégicos, promover la alfabetización digital ciudadana y articular la protección de datos con el desarrollo de la economía digital sostenible.

CONCLUSION

La Ley Orgánica de Protección de Datos Personales constituye un avance decisivo en la consolidación del Estado constitucional de derechos y justicia; sin embargo, su eficacia práctica dependerá de la capacidad institucional para fiscalizar el tratamiento masivo e invisible de datos que caracteriza al denominado *espacio de los flujos*. La expansión de los servicios *fintech* y la migración a infraestructuras en la nube exigen fortalecer los protocolos de seguridad, anonimización y gobernanza,



así como armonizar las transferencias internacionales con estándares tales como el RGPD y el Convenio 108+. La experiencia pandémica, por su parte, evidenció que la invocación del interés público no puede convertirse en vía libre para la vulneración de la intimidad, lo que hace imperativa la existencia de salvaguardias rigurosas y de una supervisión ex post efectiva. De cara al futuro, la adopción de enfoques *privacy-by-design*, la alfabetización digital ciudadana y la coordinación interinstitucional resultan indispensables para equilibrar la innovación tecnológica con la tutela efectiva de la autodeterminación informativa; solo así se garantizará que el progreso digital redunde en un desarrollo social inclusivo y respetuoso de los derechos fundamentales en el Ecuador.

FINANCIAMIENTO

No monetario

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A la dirección de investigación de la Universidad Regional Autónoma de los Andes.

REFERENCIAS

- Bonfield, C. A., Salter, M., Longmuir, A., Benson, M., & Adachi, C. (2020). Transformation or evolution?: Education 4.0, teaching and learning in the digital age. *Higher Education Pedagogies*, 5(1), 223–246.
- Castells, M. (2020). Space of flows, space of places: Materials for a theory of urbanism in the information age. In *The city reader* (pp. 240–251). Routledge.
- Gabor, D., & Brooks, S. (2020). The digital revolution in financial inclusion: International development in the fintech era. In *Material cultures of financialisation* (pp. 69–82). Routledge.
- Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine*, 26(4), 463–464.
- Keesara, S., Jonas, A., & Schulman, K. (2020). Covid-19 and health care's digital revolution. *New England Journal of Medicine*, 382(23), e82.
- Kumar, V., Ramachandran, D., & Kumar, B. (2021). Influence of new-age technologies on marketing: A research agenda. *Journal of Business Research*, 125, 864–877.
- Lee, S. M., & Lee, D. (2020). "Untact": A new customer service strategy in the digital age. *Service Business*, 14(1), 1–22.



- Libai, B., Bart, Y., Gensler, S., Hofacker, C. F., Kaplan, A., Kötterheinrich, K., & Kroll, E. B. (2020). Brave new world? On AI and the management of customer relationships. *Journal of Interactive Marketing*, 51(1), 44–56.
- Parker, S. K., & Grote, G. (2022). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. *Applied Psychology*, 71(4), 1171–1204.
- Pencarelli, T. (2020). The digital revolution in the travel and tourism industry. *Information Technology & Tourism*, 22(3), 455–476.
- Rachmad, Y. E. (2024). *The future of influencer marketing: Evolution of consumer behavior in the digital world*. PT. Sonpedia Publishing Indonesia.
- Romansky, R. (2022). Digital age and personal data protection. *International Journal on Information Technologies & Security*, 14(3), 89–100.
- Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17(5), 5288–5303.
- Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in data protection and artificial intelligence: Trends and challenges. *International Journal of Advanced Engineering Technologies and Innovations*, 1(1), 294–319.
- Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, 8, 131723–131740.

Derechos de autor: 2024 Por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0)

<https://creativecommons.org/licenses/by-nc-sa/4.0/>