sensors

MDPI

Type of the Paper (Article, Review, Communication, etc.)

Comparación de derechos informáticos en Ecuador y el mundo

Karla Mayerlin Almea Velez [1], Tommy Steeven Apolinario Sánchez [2]

[1] Universidad Técnica Estatal de Quevedo 1; [kalmeav, tommy.apolinario2018]@uteq.edu.ec

Abstract: Este estudio analiza los derechos informáticos en Ecuador, comparando su marco normativo (Ley Orgánica de Protección de Datos Personales, COIP, EGSI 2024) con estándares internacionales como el RGPD y la CCPA. Mediante revisión documental y análisis cualitativo, se identifican avances en protección de datos y tipificación de delitos digitales, pero también brechas críticas: falta de armonización con estándares globales, sanciones insuficientes para ciberdelitos complejos y desafíos en implementación práctica de políticas de ciberseguridad, agravados por desigualdad en acceso a tecnología y baja alfabetización digital. El artículo propone fortalecer el marco legal mediante actualizaciones al COIP, inversión en capacitación técnica y cooperación regional alineada con iniciativas como la Estrategia Interamericana de Ciberseguridad de la OEA, ofreciendo un enfoque integral para mejorar la protección de derechos digitales en un contexto globalizado.

Keywords: Derechos informáticos, protección de datos, ciberseguridad, Ecuador, normativa internacional.

1. Introducción

En la actualidad, la regulación de los derechos informáticos es uno de los factores que presenta relevancia en la era digital, puesto que garantiza la seguridad, privacidad y el acceso a la información a nivel global. Ecuador, al igual que muchas naciones, ha desarrollado un marco normativo que aborda aspectos como la protección de datos personales, la ciberseguridad y los delitos informáticos. Sin embargo, los avances de las telecomunicaciones e informática traen consigo un conjunto de desafíos que deben ser considerados en las normativas [1].

En el estudio realizado por Moreira, et al. [2] se destaca la necesidad de mejorar la educación y la concientización con respecto a la importancia de la seguridad informática en Ecuador, subrayando que es crucial que las personas y organizaciones tomen medidas preventivas para protegerse de delitos informáticos. Además, se ha señalado que las sanciones definidas en el Código Orgánico Integral Penal (COIP) no es suficiente para abarcar la diversidad de delitos que se cometen a diario, lo que indica que es necesario fortalecer la legislación existente [3], [1].

A nivel internacional, la protección de los derechos informáticos varía considerablemente. Mientras que en algunos países se han implementado normativas y legislaciones actualizadas, otros enfrentan problemas en la adaptación de sus marcos legales debido a las nuevas realidades digitales. Esta variabilidad en la regulación se relaciona con la discusión sobre el consenso y desacuerdo en el ámbito legal, donde juristas pueden tener diferentes interpretaciones sobre cómo abordar problemas emergentes dentro del marco del derecho [4]. La comparación que se presenta en este trabajo permitirá identificar áreas de mejora y adoptar mejores prácticas que fortalezcan la protección de los derechos informáticos en Ecuador.

Este artículo tiene como objetivo analizar y comparar los derechos informáticos en Ecuador con los marcos normativos de otras naciones, identificando similitudes, diferencias y áreas de mejora. Para ello, se considerarán aspectos como la legislación de la protección de datos, regulación de la ciberdelincuencia y derechos digitales en el contexto global, proporcionando un análisis sobre la evolución y los desafíos de los derechos informáticos en el país frente a estándares internacionales.

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Received: date
Revised: date
Accepted: date
Published: date

2. Marco teórico

2.1. Conceptos Fundamentales de Derechos Informáticos

El derecho informático se refiere al conjunto de normas y principios que regulan el uso, acceso, protección y gestión de la información en entornos digitales. Este derecho incluye, entre otros, la protección de datos personales, la seguridad informática, la privacidad digital y el acceso a la información. En un mundo cada vez más interconectado, estos derechos son esenciales para garantizar la confianza en las tecnologías de la información y la comunicación (TIC) [5]. Para fin de mantener la claridad en este trabajo, se mencionan algunos de los conceptos más importantes:

- **Protección de Datos Personales:** Se refiere al derecho de los individuos a controlar cómo se recopilan, almacenan y utilizan sus datos personales. Este concepto ha ganado relevancia con el auge de las plataformas digitales y la economía basada en datos [6].
- **Ciberseguridad:** Abarca las medidas técnicas y legales para proteger sistemas informáticos, redes y datos de accesos no autorizados, ataques cibernéticos y otros riesgos digitales [7].
- **Privacidad Digital:** Garantiza que los individuos puedan mantener el control sobre su información personal en línea, incluyendo su comunicación y actividades digitales [8].
- **Acceso a la Información:** Se refiere al derecho de los ciudadanos a acceder a información pública y a servicios digitales, promoviendo la transparencia y la inclusión digital [9].
- **Cibercrimen:** Conjunto de actividades ilícitas que se realizan mediante el uso de sistemas informáticos e internet. Esto incluye delitos como el acceso no autorizado a sistemas, el robo de datos, el fraude electrónico, y ataques dirigidos a infraestructuras críticas, entre otros [10].

2.2. Marco Normativo Internacional

Dentro de las normativas internacionales de derechos informáticos han existido cambios significativos en las últimas décadas, impulsado por la creciente digitalización de la sociedad y la necesidad de regular el uso de las TIC [11]. El marco normativo internacional, es decir, el conjunto de tratados, convenios, regulaciones y estándares globales busca armonizar las legislaciones nacionales, proteger los derechos de los usuarios y fomentar la cooperación entre países en temas como la protección de datos personales, la ciberseguridad y la lucha contra la ciberdelincuencia [12].

Una de las herramientas más destacadas a nivel internacional es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, aprobado en 2018. Este reglamento establece un estándar global en materia de protección de datos personales, aplicable no solo a los países miembros de la UE, sino también a cualquier organización que maneje datos de ciudadanos europeos. El RGPD se basa en principios como el consentimiento explícito, la transparencia, la minimización de datos y el derecho al olvido, y ha servido como modelo para muchas legislaciones nacionales en todo el mundo. Su impacto ha sido tan significativo que ha llevado a empresas y gobiernos a reevaluar sus prácticas de manejo de datos [13].

La Organización de los Estados Americanos (OEA) ha jugado un papel importante en la promoción de estándares regionales en ciberseguridad y protección de datos. Mediante iniciativas como la Estrategia Interamericana de Ciberseguridad, la OEA busca fomentar la cooperación entre sus miembros para fortalecer las capacidades nacionales en la prevención y respuesta a incidentes cibernéticos [14]. Además, ha desarrollado guías y recomendaciones para la implementación de políticas públicas en materia de derechos informáticos, refiriéndose específicamente a las estrategias nacionales de ciberseguridad que incluyen la adopción de marcos regulatorios, protocolos de respuesta a incidentes y

medidas para la protección de datos e infraestructuras críticas, aunque su adopción varía significativamente entre los países miembros [15].

Por otro lado, en Estados Unidos, la Ley de Privacidad del Consumidor de California (CCPA), implementada en 2020, aunque no es una normativa federal, su influencia ha sido considerable. La CCPA otorga a los consumidores derechos similares a los del RGPD, como el acceso a sus datos, la posibilidad de solicitar su eliminación y la opción de optar por no compartir su información con terceros [16].

Además de estas normativas específicas, organismos internacionales como la Organización de las Naciones Unidas (ONU) y la Unión Internacional de Telecomunicaciones (UIT) han trabajado en la promoción de estándares globales para garantizar un entorno digital seguro y accesible. La ONU, por ejemplo, ha reconocido el acceso a Internet como un derecho humano y ha impulsado iniciativas para reducir la brecha digital, especialmente en países en desarrollo [17]. Por su parte, la UIT ha desarrollado estándares técnicos y normativos para la seguridad de las comunicaciones digitales, promoviendo la adopción de buenas prácticas a nivel global [18].

El marco normativo internacional en derechos informáticos es amplio y diverso, con instrumentos como el RGPD y la CCPA liderando los esfuerzos globales en protección de datos y ciberseguridad [19]. Sin embargo, la implementación efectiva depende de la voluntad política de los países y de su capacidad para adaptarse a los rápidos cambios tecnológicos [20]. Aunque se han logrado avances significativos, persisten desafíos importantes, como la falta de armonización entre legislaciones nacionales y la necesidad de fortalecer la cooperación internacional en un mundo cada vez más interconectado.

3. Comparativa de legislación ecuatoriana con el resto del mundo

Para llevar a cabo este estudio comparativo, se empleará una metodología cualitativa basada en una revisión documental y el análisis de las legislaciones de diferentes naciones. A continuación, se presentan los pasos a seguir:

1. **Recolección de información:** Para analizar y compara las regulaciones informáticas aplicadas en otros países y Ecuador, se recopilarán documentos legales, leyes, reglamentos y directrices. Las fuentes incluirán bases de datos jurídicas, publicaciones académicas y documentos oficiales.
2. **Análisis comparativo:** Se realizará un análisis de las similitudes y diferencias entre las legislaciones, enfocándose en aspectos como la protección de datos, la regulación de delitos informáticos y las políticas de ciberseguridad
3. **Conclusiones y recomendaciones:** Basándose en los hallazgos obtenidos del análisis, se elaborarán y propondrán recomendaciones para mejorar el marco normativo ecuatoriano en materia de derecho informático.

Ecuador y los derechos informáticos

Los derechos informáticos en el Ecuador han evolucionado en los últimos años con la incorporación de normativas que buscan proteger la privacidad, seguridad e integridad de los ciudadanos en el entorno digital. Para ello, en Ecuador se han desarrollado un conjunto de marcos legales relacionados con los derechos informáticos en Ecuador, estos son:

Ley Orgánica de Protección de Datos Personales

En 2021, Ecuador aprobó esta ley, que establece reglas para el uso de la información personal de los ciudadanos. Esta ley busca evitar que los datos de las personas sean utilizados sin permiso o de manera inadecuada. Para ello, introduce figuras como la Autoridad de Protección de Datos y regula el uso de datos en el sector público y privado. Su aplicación busca trabajar en armonía con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea [21].

Código Orgánico Integral Penal (COIP)

El COIP tiene una sección nombrada "SECCIÓN TERCERA: Delitos contra la seguridad de los activos de los sistemas de información y comunicación", la cual está dedicada a delitos informáticos, donde se tipifica y sanciona conductas como el acceso no autorizado a sistemas informáticos, la violación de datos personales y el fraude electrónico [22].

Ley de Comercio Electrónico, Firmas y Mensajes de Datos

Esta ley regula la validez jurídica de los documentos electrónicos y la certificación de las firmas digitales, fue publicada en el año 2002. Permite que los documentos digitales tengan la misma validez que los documentos físicos o en papel, para así facilitar las transacciones en línea en el país [23].

Esquema Gubernamental de Seguridad de la Información (EGSI)

La primera versión de este esquema fue publicada en 2013. La misma establece directrices para la protección de datos en entidades gubernamentales y el fortalecimiento de la ciberseguridad. Este esquema se encuentra en su tercera versión (publicado en 2024) y está estructurado considerando tres guías, que son [24]:

- Guía para la implementación del EGSI, basado en la NTE INEN ISO/IEC 27001.
- Guía para la gestión de riesgos de seguridad de la información, basado en NTE INEN ISO/IEC 27005 y la metodología MAGERIT.
- Guía para la implementación de controles de seguridad de la información, basado en NTE INEN ISO/IEC 27002.

Es decir, en Ecuador se han definido un conjunto de normativas que busca garantizar los derechos informáticos. A continuación, se presenta una tabla comparativa entre los cuatro reglamentos previamente especificados.

Normativa	Descripción	Objetivo	Aplicación
Ley Orgánica de Protección de Datos Personales	Regula el uso de la información personal de los ciudadanos. Obliga a las empresas y entidades públicas a garantizar la privacidad de los datos	Proteger los datos personales y evitar su uso indebido	Empresas, entidades públicas y cualquier organización que maneje datos personales.
Código Orgánico Integral Penal (COIP)	Define y sanciona los delitos cometidos haciendo uso de tecnologías digitales, como el acceso no autorizado a sistemas, robo de datos y fraude electrónico	Sancionar delitos informáticos y proteger a los usuarios de ataques cibernéticos	Aplica a cualquier persona que cometa delitos informáticos en Ecuador.
Ley de Comercio Electrónico, Firmas y Mensajes de Datos	Regula las transacciones electrónicas y digitales, brindándoles validez legal	Garantizar la seguridad y validez del comercio digital y la documentación electrónica	Empresas, instituciones financiaras y ciudadanos que realicen transacciones en línea o digitales
Esquema Gubernamental de Seguridad de la Información (EGSI)	Establece normas para la protección de la información de entidades gubernamentales, con el fin de prevenir filtraciones y ataques cibernéticos	Asegurar que el sector público mantenga estándares adecuados de seguridad informática	Instituciones estatales y servidores públicos

Sin embargo, existen publicaciones realizadas que indican que las normativas que posee el Ecuador no son suficientes para sancionar a las personas que cometen crímenes digitales o no respetan los derechos informáticos. Sarasti [25] examina la relación entre los derechos constitucionales, humanos y las tecnologías de la información en Ecuador, destacando a pesar de la existencia de un marco legal que promueve este acceso, persisten desafíos como la desigualdad en el acceso a las TIC, la falta de cobertura y la alfabetización digital. Asimismo, Moreira [2] sugiere que, para garantizar una protección adecuada de los derechos de propiedad intelectual y la seguridad de la información es necesario regular el derecho informático y la protección de datos en Ecuador, es necesario implementar y aplicar estas leyes. Por su parte, Juca & Medina [20] mencionan que las normativas detalladas en los reglamentos existentes son válidas, pero se requiere de una mayor inversión y capacitación en TIC y ciberseguridad.

Leyes internacionales

Para comparar las normativas ecuatorianas con las internacionales, en esta sección se especifican algunos de los reglamentos internacionales.

Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, adoptado en 2016 y en vigor desde 2018, es considerado uno de los marcos normativos más avanzados en materia de protección de datos personales a nivel mundial. Su aplicación se extiende no solo a los países miembros de la UE, sino también a cualquier organización que procese datos de ciudadanos europeos, independientemente de su ubicación geográfica [26].

Principios Fundamentales del RGPD

El RGPD se basa en una serie de principios fundamentales que regulan el tratamiento de los datos personales:

- Licitud, lealtad y transparencia: Los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Limitación de la finalidad: Los datos solo pueden ser recopilados para fines específicos, explícitos y legítimos.
- Minimización de datos: Se debe garantizar que los datos personales sean adecuados, pertinentes y limitados a lo necesario para los fines del tratamiento.
- Exactitud: Los datos deben ser exactos y, cuando sea necesario, actualizados.
- Limitación del plazo de conservación: Los datos deben conservarse durante un período no mayor al necesario para los fines del tratamiento.
- Integridad y confidencialidad: Se deben aplicar medidas de seguridad adecuadas para proteger los datos personales frente a accesos no autorizados o ilícitos [26].

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP), aprobada en 2021, establece principios similares a los del RGPD, aunque con ciertas diferencias clave:

- Alcance Territorial: Mientras que el RGPD se aplica a cualquier entidad que trate datos de ciudadanos europeos, la LOPDP se limita al territorio ecuatoriano, sin una disposición clara sobre el tratamiento de datos de extranjeros por entidades ecuatorianas.
- Autoridad de Control: El RGPD establece autoridades independientes en cada Estado miembro con amplios poderes de sanción, mientras que en Ecuador la supervisión está a cargo de la Superintendencia de Protección de Datos, cuya autonomía y capacidades aún están en proceso de consolidación.

- Sanciones: En la UE, las multas por incumplimiento del RGPD pueden alcanzar hasta el 4% de la facturación global de una empresa, mientras que en Ecuador las sanciones económicas son menores y con menor grado de aplicación hasta la fecha.
- Derechos de los Ciudadanos: Ambos marcos garantizan derechos como el acceso, rectificación, supresión y portabilidad de datos. Sin embargo, el RGPD otorga un mayor énfasis en el derecho al olvido, permitiendo que los ciudadanos soliciten la eliminación de sus datos de manera más efectiva [26].

Convenio sobre Cibercriminalidad (Convención de Budapest)

El Convenio sobre Cibercriminalidad, también conocido como Convención de Budapest, es el primer tratado internacional diseñado para abordar los delitos informáticos y mejorar la cooperación internacional en la lucha contra la cibercriminalidad. Adoptado por el Consejo de Europa en 2001 y en vigor desde 2004, este convenio establece estándares para la tipificación de delitos informáticos y proporciona mecanismos para la colaboración transnacional [27].

Principales Aspectos del Convenio

- Tipificación de delitos informáticos: Define como ilícitos el acceso no autorizado a sistemas, la interferencia en datos y sistemas, la falsificación informática y el fraude informático.
- Medidas de cooperación internacional: Promueve la asistencia mutua entre países para la investigación y persecución de delitos informáticos.
- Procedimientos para la obtención de evidencia digital: Establece normas para la preservación rápida de datos y el acceso a información transfronteriza.
- Protección de derechos humanos y privacidad: Equilibra la persecución del delito con el respeto a los derechos fundamentales de los ciudadanos [28].

Comparación con la Legislación de Ecuador

Ecuador ha desarrollado normativas relacionadas con la cibercriminalidad, pero su adhesión a estándares internacionales aún enfrenta desafíos clave:

- Marco normativo: Aunque Ecuador penaliza ciertos delitos informáticos en el Código Orgánico Integral Penal (COIP), la legislación no se encuentra completamente alineada con la Convención de Budapest.
- Cooperación internacional: Mientras que el convenio establece protocolos claros para la colaboración entre países, Ecuador carece de mecanismos específicos y acuerdos formales con múltiples naciones en la lucha contra la cibercriminalidad.
- Capacidades de investigación y enjuiciamiento: La Convención de Budapest enfatiza el desarrollo de capacidades especializadas para el rastreo y análisis de delitos informáticos, algo que en Ecuador todavía se encuentra en proceso de fortalecimiento [28] [1].

Ley de Privacidad del Consumidor de California (CCPA)

La Ley de Privacidad del Consumidor de California (CCPA), vigente desde 2020, establece derechos de privacidad sólidos para los consumidores y obligaciones estrictas para las empresas que manejan datos personales. Esta ley otorga a los

ciudadanos de California el derecho a conocer qué datos personales se recopilan, solicitar su eliminación y optar por no vender su información [29].

Comparación con la Legislación de Ecuador

- Derechos del consumidor: Similar a la LOPDP, la CCPA otorga a los consumidores derechos sobre sus datos personales, pero con una regulación más estricta en la comercialización de datos.
- Multas y sanciones: La CCPA impone multas severas por incumplimiento, algo que Ecuador aún debe fortalecer en su legislación [29].

Ley de Protección de Datos Personales de Brasil (LGPD)

La Ley General de Protección de Datos Personales de Brasil (LGPD), aprobada en 2018 y en vigor desde 2020, establece un marco regulatorio integral para la protección de datos personales en Brasil. Similar al RGPD, esta ley tiene como objetivo garantizar la privacidad y seguridad de la información personal de los ciudadanos [30].

Principales Aspectos de la LGPD

- Aplicación extraterritorial: La LGPD se aplica a cualquier organización que procese datos personales en Brasil o de ciudadanos brasileños, incluso si la empresa no tiene presencia física en el país.
- Derechos de los titulares de los datos: Los ciudadanos tienen derecho a acceder, corregir, eliminar, restringir el procesamiento y solicitar la portabilidad de sus datos.
- Base legal para el procesamiento de datos: La LGPD permite el tratamiento de datos bajo varias bases legales, incluida la ejecución de contratos, el cumplimiento de obligaciones legales y el consentimiento explícito del titular.
- Seguridad y prevención: Exige que las empresas implementen medidas de seguridad adecuadas para proteger los datos personales contra accesos no autorizados y fugas de información [30].

Comparación con la Legislación de Ecuador

- Alcance: Mientras que la LGPD se aplica a cualquier empresa que maneje datos de brasileños, la LOPDP en Ecuador no establece claramente el tratamiento de datos de extranjeros por parte de entidades ecuatorianas [31].
- Sanciones: La LGPD impone multas de hasta el 2% del ingreso anual de la empresa, con un límite de 50 millones de reales por infracción, mientras que las sanciones en Ecuador aún son menos severas en comparación [30].
- Autoridad Reguladora: Brasil cuenta con la Autoridad Nacional de Protección de Datos (ANPD), un organismo autónomo responsable de la supervisión y cumplimiento de la LGPD, mientras que en Ecuador esta labor recae en la Superintendencia de Protección de Datos [30].

Objetivos y Principales Disposiciones

El convenio busca armonizar las legislaciones nacionales, establecer mecanismos de cooperación internacional y mejorar las herramientas procesales para la investigación y enjuiciamiento de delitos cometidos en entornos digitales. Entre los delitos tipificados en la convención se incluyen:

- Acceso ilícito a sistemas informáticos (hacking).
- Intercepción ilegal de datos.
- Interferencia en sistemas y datos informáticos.
- Fraude informático y falsificación de datos.

- Distribución de material ilícito, incluyendo la pornografía infantil.
- Violaciones a los derechos de autor en entornos digitales [32].

La convención también establece procedimientos específicos para la recolección de pruebas electrónicas y el acceso a datos almacenados en sistemas informáticos. Esto incluye la preservación expedita de información, el acceso a tráfico de datos en tiempo real y el acceso transfronterizo a información bajo ciertas condiciones [32].

4. Resultados

El análisis comparativo de los marcos normativos sobre derechos informáticos en Ecuador y otras jurisdicciones ha permitido identificar fortalezas y debilidades en la legislación ecuatoriana. En términos de protección de datos personales, la Ley Orgánica de Protección de Datos Personales (LOPDP) muestra avances significativos al alinearse con principios del RGPD, aunque su implementación aún enfrenta desafíos en términos de supervisión y sanción efectiva. A diferencia del RGPD y la LGPD de Brasil, la LOPDP no cuenta con una autoridad de control plenamente consolidada, lo que limita su capacidad de hacer cumplir las normativas.

En el ámbito de la ciberseguridad y delitos informáticos, Ecuador ha tipificado varias infracciones en el Código Orgánico Integral Penal (COIP), pero no cuenta con un marco legal robusto para la persecución del cibercrimen a nivel internacional. En contraste, el Convenio de Budapest establece directrices claras para la cooperación entre países, facilitando el intercambio de información y la asistencia mutua. La falta de adhesión de Ecuador a este tratado representa una barrera para enfrentar delitos cibernéticos transnacionales de manera efectiva.

Por otro lado, la Ley de Privacidad del Consumidor de California (CCPA) presenta un enfoque más estricto en la comercialización de datos y en la capacidad de los consumidores para optar por no compartir su información personal con terceros. En Ecuador, si bien la LOPDP reconoce derechos similares, su aplicación es más flexible y carece de mecanismos eficientes para hacer cumplir la normativa en entornos digitales altamente comercializados.

Además, el análisis del Explanatory Report to the Convention on Cybercrime (ETS No. 185) destaca la importancia de la armonización legal y la cooperación internacional para combatir delitos informáticos. La falta de infraestructura especializada y la limitada capacitación en ciberseguridad en Ecuador representan desafíos clave para la adopción de normativas más efectivas en este campo.

5. Conclusiones

A partir de la comparación de los marcos regulatorios analizados, se concluye que Ecuador ha dado pasos importantes en la protección de derechos informáticos, pero aún enfrenta desafíos en la implementación efectiva de sus normativas. Las principales conclusiones de este estudio son:

1. Necesidad de fortalecer la autoridad de control: La Superintendencia de Protección de Datos debe consolidarse como un organismo autónomo con mayores recursos y facultades sancionadoras para garantizar la efectiva protección de datos personales.
2. Mejor alineación con estándares internacionales: La adhesión de Ecuador al Convenio de Budapest mejoraría la cooperación internacional en la lucha contra el cibercrimen y facilitaría la modernización de sus herramientas de investigación digital.
3. Aumento en la capacidad de supervisión y sanción: Comparado con el RGPD y la CCPA, Ecuador aún carece de sanciones significativas

para incumplimientos en protección de datos, lo que reduce la efectividad de la normativa.

4. Capacitación y sensibilización en derechos digitales: Se requiere una mayor inversión en educación digital y ciberseguridad, tanto para ciudadanos como para organismos estatales y empresas privadas.
5. Mejora en la cooperación con el sector privado: La protección de derechos informáticos debe ir acompañada de acuerdos con el sector tecnológico y financiero para establecer mejores prácticas en seguridad y privacidad.

Referencias

[1] F. Juca-Maldonado and R. Medina-Peña, "Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.," *Portal de la Ciencia*, vol. 4, no. 3, pp. 325–337, Sep. 2023, doi: 10.51247/pdlc.v4i3.394.

[2] I. A. Moreira Moreira, M. Navia Mendoza, and J. Parraga-Alava, "El derecho informático y la influencia en los sistemas de información: un análisis bibliográfico bajo la perspectiva jurídica y tecnológica en Ecuador," *Revista Tecnológica - ESPOL*, vol. 36, no. 1, pp. 162–178, Jun. 2024, doi: 10.37815/rte.v36n1.1151.

[3] S. G. Tixi-Janeta, M. L. Merizalde-Avilés, A. J. Romero-Fernández, and G. V. Jordán-Naranjo, "Los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano," *IUSTITIA SOCIALIS*, vol. 8, no. 1, pp. 1610–1619, Sep. 2023, doi: 10.35381/racji.v8i1.3339.

[4] B. Watson, "Explaining legal agreement," *Jurisprudence*, vol. 14, no. 2, pp. 221–253, Apr. 2023, doi: 10.1080/20403313.2023.2165789.

[5] Z. Ma, S. Zhang, X. Li, J. Guo, L. Yang, and S. Cao, "Can the new model of shared property rights promote better corporate financial performance in China?," *Financial Innovation*, vol. 11, no. 1, p. 75, Feb. 2025, doi: 10.1186/s40854-024-00725-0.

[6] R. Zhu, M. Wang, X. Zhang, and X. Peng, "Investigation of personal data protection mechanism based on blockchain technology," *Sci Rep*, vol. 13, no. 1, p. 21918, Dec. 2023, doi: 10.1038/s41598-023-48661-w.

[7] SAHIL HUSEN SHAIKH, ANIKET PANDURANG DATIR, and ABHISHEK SATISH BIRAJDAR, "Cyber Security in the Age of Digital Transformation," *IRE Journals*, vol. 7, no. 12, Jun. 2024.

[8] B. Song, M. Deng, S. R. Pokhrel, Q. Lan, R. Doss, and G. Li, "Digital Privacy Under Attack: Challenges and Enablers," Feb. 2023.

[9] A. Yannoukakou and I. Araka, "Access to Government Information: Right to Information and Open Government Data Synergy," *Procedia Soc Behav Sci*, vol. 147, pp. 332–340, Aug. 2014, doi: 10.1016/j.sbspro.2014.07.107.

[10] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, "Cybersecurity and cybercrime: Current trends and threats," *JOURNAL OF INTERNATIONAL STUDIES*, vol. 17, no. 2, pp. 220–239, Jun. 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[11] R. Uerpmann-Wittzack, "Principles of International Internet Law," *German Law Journal*, vol. 11, no. 11, pp. 1245–1263, Nov. 2010, doi: 10.1017/S2071832200020204.

[12] G. S. Bajpai, "Analyzing the Evolution of Cyber Law: A Comprehensive Review of Data Protection and Privacy Regulations," *Indian Journal of Law*, vol. 2, no. 4, pp. 85–90, Aug. 2024, doi: 10.36676/ijl.v2.i4.46.

[13] L. Puljak, A. Mladinić, and Z. Koporc, "Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study," *BMC Res Notes*, vol. 16, no. 1, p. 41, Mar. 2023, doi: 10.1186/s13104-023-06308-z.

[14] F. Radoniewicz, "International Regulations of Cybersecurity," in *Cybersecurity in Poland*, Cham: Springer International Publishing, 2022, pp. 53–71. doi: 10.1007/978-3-030-78551-2_5.

[15] A. T. Odebade and E. Benkhelifa, "A Comparative Study of National Cyber Security Strategies of ten nations," Mar. 2023.

[16] California Privacy Protection Agency, "Ley de Privacidad del Consumidor de California (CCPA)," Laws & Regulations.

[17] Anne-Marie Grey, "En apoyo a la conectividad: el nuevo derecho humano," DÍA DE LOS DERECHOS HUMANOS.

[18] S. Klotz, "Who drives the international standardisation of telecommunication and digitalisation? Introducing a new data set," *Glob Policy*, vol. 14, no. 3, pp. 558–568, Jun. 2023, doi: 10.1111/1758-5899.13223.

[19] A. Tsohou *et al.*, "Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform," *Information & Computer Security*, vol. 28, no. 4, pp. 531–553, Apr. 2020, doi: 10.1108/ICS-01-2020-0002.

[20] P. Dewitte and J. Ausloos, "Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead," Feb. 27, 2024. doi: 10.31219/osf.io/sk34h.

[21] Asamblea Nacional del Ecuador, "Ley Orgánica de Protección de Datos Personales," Ecuador, May 2021.

[22] Asamblea Nacional del Ecuador, *Código Orgánico Integral Penal (COIP)*. 2014.

[23] Asamblea Nacional del Ecuador, *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. 2002.

[24] Secretaría Nacional de Gestión de la Política, "Esquema Gubernamental de Seguridad de la Información (EGSI)," Ecuador, Mar. 2024.

[25] P. A. Sarasti, "Constitutional Rights, Human Rights and Information and Communication Technologies in Ecuador," *Migration Letters*, vol. 20, no. S10, pp. 1150–1158, Nov. 2023, doi: 10.59670/ml.v20iS10.5493.

[26] Parlamento Europeo, *Reglamento General de Protección de Datos (RGPD)*. 2016.

[27] Instituto Nacional de Ciberseguridad de España (INCIBE), "Informe sobre ciberseguridad en América Latina y el Caribe," 2021.

[28] "BOE-A-2010-14221 Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001." Accessed: Feb. 10, 2025. [Online]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[29] U.S. Congress, *California Consumer Privacy Act (CCPA)*. 2018.

[30] Gobierno de Brasil, *Lei Geral de Proteção de Dados Pessoais (LGPD)*. 2018.

[31] Asamblea Nacional del Ecuador, "Ley de Comercio Electrónico, Firmas y Mensajes de Datos," Ecuador, Apr. 2002.

[32] "Explanatory Report to the Convention on Cybercrime".

Anexos