REVISTA CIENTÍFICA
CONECTIVIDAD
Instituto Superior Tecnológico Universitario Rumiñahui

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

Artículo Científico

Análisis comparado sobre la protección tecnológica y social de los datos personales en el Ecuador

Comparative analysis on the technological and social protection of personal data in Ecuador

María Isabel Jaramillo Vargas[1]

[1] Universidad Católica de Santa Fe, m_isajaramillo@yahoo.es, Santa Fe, Argentina

Autor para correspondencia: m_isajaramillo@yahoo.es

RESUMEN

Ecuador aprobó la Ley Orgánica de Protección de Datos Personales en 2021; Colombia tiene la Ley 1.581 de 2012; Perú, la Ley 29.733; Chile modernizó la Ley 19.628 de 1999 mediante recientes actualizaciones; todas las normas mencionadas están destinadas a proteger la identidad digital de la ciudadanía; la metodología aplicada, se sustenta en el método analítico, que implica descomponer cada uno de los textos en sus partes esenciales para comprenderlos de manera crítica, profunda e integral, descubriéndose brechas tecnológicas entre países; por ejemplo Colombia y Perú, tienen sistemas de notificación de vulneraciones y certificación de cumplimiento implementados, mientras que Ecuador no cuenta con la infraestructura técnica suficiente; en lo social, hay menos conocimiento por parte de los ciudadanos ecuatorianos sobre los derechos digitales en comparación con Chile, donde se ha desarrollado una cultura de protección de datos; otro factor importante es la implementación de leyes ARCO : Colombia y Perú presentan plataformas digitales eficientes para el efecto, mientras que Ecuador recién inicia su implementación; además, países como Chile y Colombia establecen sanciones como medidas de disuasión ante cualquier ataque y vulneración; mientras que Ecuador, es laxo en este sentido.

Palabras clave: Vulneraciones; Método analítico; Certificaciones; Derechos digitales; Sistemas.

ABSTRACT

Ecuador approved the Organic Law on Personal Data Protection in 2021; Colombia has Law 1,581 of 2012; Peru, Law 29,733; Chile modernized Law 19,628 of 1999 through recent updates; all of the aforementioned regulations are intended to protect citizens' digital identities; the methodology applied is based on the analytical method, which involves breaking down each of the texts into their essential parts to understand them critically, in-depth, and comprehensively, uncovering technological gaps between countries. For example, Colombia and Peru have systems for reporting violations and certifying compliance implemented, while Ecuador lacks sufficient technical infrastructure. Socially, Ecuadorian citizens are less aware of digital rights compared to Chile, where a culture of data protection has developed. Another important factor is the implementation of ARCO laws: Colombia and Peru have efficient digital platforms for this purpose, while Ecuador is just beginning to implement them. Furthermore, countries like Chile and Colombia establish sanctions as deterrent measures against any attack or violation; while Ecuador is lax in this regard.

Keywords: Violations; Analytical method; Certifications; Digital rights; Systems.

[1]Acceso, Rectificación, Cancelación y Oposición de datos personales

Citas

Jaramillo Vargas, M. (2025). Análisis comparado sobre la protección de datos personales en el Ecuador. CONECTIVIDAD, 6(3). https://doi.org/10.37431/conectividad.v6i3.309

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

1. INTRODUCCIÓN

El presente artículo se busca establecer el grado de desarrollo social y aplicación a nivel tecnológico de la Ley Orgánica de Protección de Datos Personales del Ecuador en relación a otras experiencias de países sudamericanos vecinos como Colombia, Perú y Chile, que tienen una normativa de mayor tiempo de aplicación en sus territorios.

Desde el punto de vista tecnológico, el presente análisis de tipo comparativo, demuestra las falencias en la infraestructura digital ecuatoriana para la protección de datos, como la inexistencia de un sistema automatizado de notificación de violaciones, que si se puede encontrar en Colombia y Perú; en este sentido, la propuesta de este estudio es identificar ese hito tecnológico necesario para la implementación efectiva de la legislación ecuatoriana y trazar una hoja de ruta para el desarrollo de plataformas digitales que permitan ejercer los derechos ARCO, replicando, en lo posible, las experiencias exitosas de los países vecinos.

Desde una perspectiva humanística y social, esta investigación revela cómo la tardía adopción de normativas en Ecuador ha llevado a un desconocimiento de los peligros del mundo digital a los ecuatorianos; en contraste con los programas educativos en Chile que han promovido una cultura de protección de datos; este hallazgo enriquece la comprensión de cómo los marcos legales impactan en la construcción de una ciudadanía digital sólida, no sólo en países europeos, sino también en Latinoamérica, pues la relevancia interdisciplinaria de este estudio conecta el desarrollo tecnológico necesario para implementar mecanismos de protección, con las dinámicas sociales relacionadas con la apropiación y exigibilidad de derechos digitales.

Este enfoque integral ayuda a la concienciación sobre la importancia de la protección de datos, dejando de ser un reto técnico y legal, pasando a ser un proceso de innovación social, donde la tecnología debe avanzar en sintonía con las necesidades humanas y culturales de cada sociedad; el trabajo propone un marco metodológico que puede ser replicado para evaluar la fortaleza de los sistemas de protección de datos en economías emergentes, aportando así a la literatura académica sobre soberanía digital.

2. MATERIALES Y MÉTODOS

Para llevar a cabo este análisis comparativo sobre la protección tecnológica y social de los datos personales en el Ecuador, se utiliza una metodología de investigación mixta, esto significa que se combinara tanto elementos cualitativos como cuantitativos para obtener una visión más completa del fenómeno que se está estudiando.

Se eligió los cuerpos normativos de Ecuador, Chile, Colombia y Perú, para el presente análisis, por ser países vecinos que tienen algunas similitudes económicas, tecnológicas y sociales, aunque con diferencias en su desarrollo, tal como lo recomienda Morlino (2018), quien menciona que: “la comparación es más productiva cuando se realiza entre casos que comparten características estructurales pero que muestran resultados distintos”.

El estudio se fundamentará en un enfoque de investigación comparativa, siguiendo las pautas

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

que establece Sartori (1994), quien señala que la comparación sistemática ayuda a identificar tanto similitudes como diferencias entre los casos analizados, lo que facilita la comprensión de los factores que influyen en el tema estudiando; así también como menciona Pérez Luño (2017), al analizar la protección de datos personales, es crucial adoptar una perspectiva interdisciplinaria que integre aspectos jurídicos, tecnológicos y sociales, dado que este derecho s en la actualidad, se lo puede considerar como fundamental.

En el mismo marco, se lleva a cabo un estudio documental, a través de un análisis detallado del marco normativo ecuatoriano como la Constitución, la Ley Orgánica de Protección de Datos Personales (2021) y su reglamento; y, utilizando el método de análisis legal; además del examen de las normativas de los países mencionados, se llevará a cabo un estudio de jurisprudencia nacional e internacional pertinente, así como de informes técnicos y políticas públicas

De acuerdo con Piovani & Krawczyk (2021), quienes subrayan que los estudios comparativos establecen vínculos entre variables; a continuación, se muestran las dimensiones y variables que se definirán.

Dimensión normativa: Marco constitucional de protección, legislación específica y su desarrollo, autoridades de control y sus capacidades, sanciones y mecanismos de cumplimiento e implementación del habeas data en las diversas legislaciones.

Dimensión tecnológica: Estándares técnicos exigidos, medidas de seguridad implementadas, evaluaciones de impacto, certificaciones y auditorías y notificación de brechas de seguridad

Dimensión social: Conocimiento ciudadano sobre derechos digitales, formación profesional especializada, participación de la sociedad civil y cultura organizacional de privacidad.

Para examinar los marcos normativos, se empleará el enfoque de análisis de contenido sugerido por Camps y Mujija (2008), que se fundamenta en examinar textos, discursos, imágenes y otros tipos de comunicación con el objetivo de identificar patrones, significados y estructuras subyacentes.

De igual manera, Flyvbjerg (2011) advierte que pueden existir restricciones en el estudio, como son las dificultades el acceso a datos oficiales entre naciones, la rápida evolución de las regulaciones y retos de comparabilidad a causa de las diferencias culturales.

La metodología descrita permitirá llevar a cabo un análisis riguroso y sistemático de los marcos de protección de datos personales de Ecuador, Chile, Colombia y Perú, identificando buenas prácticas, desafíos comunes y recomendaciones para fortalecer la protección de este derecho fundamental en la región andina.

3. ANÁLISIS Y DISCUSIÓN

La investigación sobre estudios desarrollados acerca de la protección de datos a nivel tecnológico y social implementados en Colombia, Perú y Chile en comparación con la legislación ecuatoriana se evidenció, lo siguiente:

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

El análisis regulatorio en Chile y su potencial impacto en Ecuador

Las debilidades en la regulación de la protección de datos personales en Chile pueden tener un impacto considerable en Ecuador, especialmente por el vínculo económico, tecnológico y migratorio entre ambos países.

A continuación, se explora cómo estas debilidades podrían influir en el desarrollo tecnológico y la protección de datos personales en Ecuador.

Debilidades regulatorias en Chile, de acuerdo con los documentos sobre "Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes" (Benucci, 2020) se identifican las siguientes debilidades regulatorias clave en Chile:

- Marco normativo desactualizado: La Ley 19.628 de 1999, aunque fue pionera en Latinoamérica, no ha recibido actualizaciones significativas para adaptarse a los avances tecnológicos de las últimas décadas (Álvarez, 2020).
- Ausencia de una autoridad de control independiente: A diferencia de otros países de la región, Chile no tiene una autoridad especializada con poderes efectivos para supervisar y sancionar (Viollier, 2017).
- Deficiencias en las obligaciones de seguridad: La normativa chilena establece obligaciones generales sin detallar medidas técnicas y organizativas específicas para proteger los datos (Cerda, 2018).
- Falta de mecanismos de notificación de brechas: No hay una obligación de informar sobre violaciones de seguridad a los afectados o a las autoridades competentes (Contreras, 2020).
- Régimen sancionatorio débil: Las sanciones económicas son demasiado leves para disuadir a las empresas, especialmente a las que manejan elevados volúmenes de información.

Implicaciones para Ecuador

- ***En el desarrollo tecnológico***

Transferencias transfronterizas de datos: Las empresas chilenas que operan en Ecuador podrían estar aplicando estándares de seguridad que no son suficientes, limitándose a cumplir con lo mínimo requerido en Chile (Remolina & Álvarez, 2018).

La falta de mecanismos para notificar brechas de seguridad representa un grave problema; pues en la actualidad, no hay obligación de informar a los afectados o a las autoridades competentes sobre violaciones de seguridad (Contreras, 2020); además, el régimen sancionatorio es bastante débil, las multas económicas no son suficientes para disuadir a las empresas u organizaciones de incumplir con la ley de protección de datos.

Desarrollo de servicios digitales: Las plataformas tecnológicas chilenas, cuyos servicios pueden llegar a Ecuador podrían estar diseñando sus servicios con arquitecturas de privacidad deficientes u obsoletas, lo que perpetúa modelos de negocio que explotan intensivamente los datos personales de los usuarios de estas plataformas.

Competitividad digital: Ecuador podría encontrarse en desventaja si decide adoptar estándares

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

más estrictos que los de Chile, puesto que esto podría ocasionar que se ahuyente inversión extranjera.

Interoperabilidad de sistemas: Las diferencias en los niveles de protección podrían complicar la colaboración en proyectos tecnológicos entre ambos países, como es el caso de los sistemas de identificación digital que son transnacionales, o los relacionados con los sistemas bancarios.

- ***En la protección social y humanística***

Desvalorización de derechos fundamentales: La influencia de las prácticas empresariales chilenas, que tienen estándares de protección bajos, podría llevar a normalizar en Ecuador un tratamiento de datos que prioriza los intereses comerciales sobre los derechos fundamentales del individuo, como es la protección de sus datos personales.

Las debilidades de la ley, detectadas en Chile podrían dificultar la armonización de los estándares de protección en la región andina, lo que complicaría la creación de un marco común que favorezca tanto la protección de derechos como el desarrollo económico de todos los países de la región, evitando que se consolide un marco común de protección.

Desafíos específicos para Ecuador

Ecuador se enfrenta al reto de encontrar un equilibrio entre atraer la inversión tecnológica de Chile, un socio comercial clave, y asegurar que se cumplan los estándares adecuados de protección de datos.

- ***Capacidad institucional:***

La Dirección Nacional de Registro de Datos Públicos de Ecuador podría tener dificultades para supervisar de manera efectiva las operaciones transfronterizas con Chile, especialmente si las prácticas de riesgo se han vuelto comunes en el ecosistema chileno.

La influencia de empresas chilenas con prácticas laxas podría socavar los esfuerzos por establecer una cultura sólida de protección de datos en la sociedad ecuatoriana.

La estrategia de Ecuador para responder a estas debilidades será crucial para garantizar que la integración tecnológica con Chile refuerce, en lugar de debilitar, la protección de los derechos fundamentales de los ciudadanos ecuatorianos en la era digital, garantizando de forma efectiva la protección de datos personales.

El análisis regulatorio en Colombia y su potencial impacto en Ecuador

Marco normativo colombiano

Colombia tiene un sistema de protección de datos personales que es bastante avanzado en comparación con otros países de América Latina, y se basa principalmente en:

- Constitución Política de Colombia (1991), como norma suprema, en su artículo 15, se reconoce de manera clara el derecho fundamental a la intimidad personal y familiar, lo que incluye el derecho al habeas data.
- Ley 1581 de 2012, Ley de Protección de Datos Personales (2012), esta ley establece el marco general para la protección de datos personales en Colombia, abarcando principios

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

fundamentales, derechos de los titulares, responsabilidades de quienes manejan los datos y los procedimientos para su implementación.

- Decreto 1377 (2013), este decreto regula parcialmente la Ley 1581, detallando aspectos como la autorización necesaria para el tratamiento de datos, las políticas de manejo de datos y cómo los titulares pueden ejercer sus derechos.
- Ley 1266 (2008), esta ley se encarga de regular el manejo de información financiera, crediticia, comercial y de servicios.
- Se establece la Superintendencia de Industria y Comercio; y a través de su Delegación para la Protección de Datos Personales, actúa como la autoridad encargada de la protección de los mismos.

Marco normativo ecuatoriano

Ecuador, a diferencia de los países vecinos, ha estado bastante rezagado en cuanto a la protección de datos personales, a pesar que la Constitución de la República del Ecuador (2008), en el artículo 66, numeral 19, reconoce el derecho a la protección de datos personales.

Después de años sin una regulación clara, Ecuador finalmente aprobó esta ley que establece principios, derechos y obligaciones en relación con el tratamiento de datos personales.

De igual manera, ha existido una falta histórica de una autoridad de control específica, actualmente para el efecto se ha designado un Superintendente de Protección de Datos Personales, con un organismo propio.

Antes de la ley mencionada, había disposiciones dispersas en diferentes normativas, como la Ley de Comercio Electrónico, la Ley Orgánica de Telecomunicaciones y el Código Orgánico Integral, pero que por el mismo hecho de constar en diversas normativas era difícil vigilar su cumplimiento y aplicación; lo que se espera que, con la vigencia de la Ley Orgánica de Protección de Datos Personales, ya no suceda.

Protección tecnológica de datos personales

Medidas tecnológicas en Colombia

Colombia ha puesto en marcha una serie de mecanismos tecnológicos para salvaguardar los datos personales de sus ciudadanos.

En primer lugar, la Superintendencia de Industria y Comercio de Colombia, impulsa estándares como ISO 27001, que se centran en la gestión de la seguridad de la información.

También, existe el Registro Nacional de Bases de Datos de Colombia, es una plataforma tecnológica que permite que tanto entidades públicas como privadas registren obligatoriamente sus bases de datos.

En Colombia, permanentemente se están implementando evaluaciones de impacto de privacidad, estas son obligatorias sobre todo para proyectos que manejan datos de alto riesgo.

Para complementar lo anterior, la Superintendencia de Industria y Comercio, ha publicado guías técnicas que ayudan a implementar medidas de seguridad en distintos sectores, con énfasis en

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

la ciudadanía.

Medidas tecnológicas en Ecuador

El avance en medidas tecnológicas en Ecuador aún está en sus primeras etapas, como se ha venido mencionando a lo largo del presente estudio, existe una ausencia histórica de estándares obligatorios, pues, hasta antes del 2021, no existía una normativa específica que exija medidas técnicas para la protección de datos.

Ecuador presenta un desarrollo incipiente de sistemas de verificación de identidad digital, no se cuenta con sistemas robustos de autenticación y verificación de identidad; los actuales son bastante limitados, y susceptibles a manipulación, pérdida o en el peor de los casos, robos de identidad.

Existe además, un desinterés incluso a nivel de Gobierno, por adoptar estándares internacionales, como ISO 27001 o el Marco de Ciberseguridad NIST (National Institute of Standards and Technology)[1] con el propósito de garantizar esta protección.

Mecanismos de cumplimiento en Ecuador

Ecuador enfrenta retos importantes en la implementación de la Ley Orgánica de Protección de Datos, entre los que se destacan:

La norma ejecutoria, es decir, el Reglamento General para la Ley Orgánica de Protección de Datos se promulgó en el año 2023; por lo tanto, aún no se ejecuta a cabalidad.

La Ley ecuatoriana, establece que debe existir una Autoridades de control, pero ésta autoridad es de reciente nombramiento; incluso el organismo estatal, es decir, la Superintendencia de Protección de Datos Personales, aún se está estructurando, por lo cual, no se puede garantizar un desempeño óptimo.

Es conocido que todo fallo judicial, debe ser debidamente motivado, en estos casos específicos, la jurisprudencia es limitada, hay pocos precedentes judiciales sobre protección de datos que guíen la aplicación de la normativa.

Finalmente, se considera que la falta de una aplicación efectiva de la Ley, se debe a la austeridad económica que atraviesa el país, pues existen restricciones presupuestarias y técnicas que dificultan la implementación de mecanismos de supervisión y control.

Implicaciones del modelo colombiano para Ecuador

El análisis del modelo colombiano, permite extraer conclusiones valiosas, que en la medida de lo posible se podrían implementar en Ecuador, con el propósito de garantizar la efectividad de la ley.

Se puede determinar que, en Colombia, la adaptación de esta norma ha sido de manera progresiva, lo que ha permitido a los sujetos obligados adaptarse paulatinamente a la misma; se podría sugerir lo mismo para Ecuador, por ejemplo, se inicie con determinados sectores estratégicos, de manera que las experiencias exitosas puedan ser replicadas a otras instituciones

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

u organismos.

Desarrollo de Guías, pues en Colombia la Superintendencia de Industria y Comercio de Colombia, impulsó el desarrollo de estos manuales, tendientes a orientar la aplicación de la Ley; lo cual se considera puede ser exitoso para Ecuador, y el organismo del ramo, empiece a publicar estos documentos como parte de esta alfabetización digital.

Además, vemos que Colombia fomenta una cultura de protección de datos que prioriza la prevención sobre la sanción, es decir, los medios coercitivos y sancionatorios constituyen el último recurso ante un incumplimiento.

Desafíos específicos para Ecuador Brecha institucional

- ***A nivel normativo e institucional***

Hay una necesidad urgente de fortalecer las capacidades institucionales, no solo a nivel estatal, sino también a nivel particular, para garantizar que se cumplan las normativas.

En primer lugar, se considera que es fundamental ajustar las regulaciones a la diversidad cultural de Ecuador, especialmente en lo que respecta a las comunidades indígenas, afrodescendientes, montubios, etc., en general trabajar con los sectores históricamente excluidos.

En segundo lugar, es importante que se desarrollen estrategias efectivas para implementar normativas en sectores donde la informalidad es alta, y no existe ningún medio de control.

Finalmente, se menciona que es crucial optimizar los recursos disponibles para asegurar que el sistema de protección de datos ecuatoriano funcione de manera efectiva.

- ***A nivel tecnológico***

A nivel de tecnologías, el Ecuador enfrenta múltiples desafíos, en relación a países vecinos y con un aparataje tecnológico de más alto nivel.

En Ecuador, es esencial desarrollar directrices claras sobre las medidas técnicas de seguridad que se adapten al contexto ecuatoriano, pues, algunas de ellas, han sido “copiadas”, del modelo europeo que este bastante avanzado en este campo.

Implementación de plataformas de registro accesibles, con sistemas de registro de bases de datos que sean fáciles de usar y económicos, de manera que se integren al sector privado en su totalidad, evitando la informalidad.

Ecuador, si desea estar a la vanguardia en el campo de la protección, debe preocuparse en crear programas de apoyo para las PYMES que faciliten la implementación de soluciones tecnológicas de protección de datos.

- ***A nivel social***

Se considera que, a nivel social, es donde falta mucho por hacer, en lo referente a la protección de datos, pues es primordial poner en marcha campañas educativas sobre derechos digitales que se dirijan a distintos sectores de la población, haciendo énfasis además en los peligros que conlleva el uso de plataformas digitales externas y la posibilidad de conceder permisos de acceso a datos personales.

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

sí mismo, se debe adaptar los mensajes, para que resulten relevantes para las diferentes étnicas y comunidades que forman el Ecuador, pues el contexto social es clave en ese sentido.

Es necesario, también, que se fomente la investigación y el diálogo sobre la protección de datos, en diversos ámbitos; pero no se quede solo a nivel local, sino que trascienda a nivel nacional e internacional.

Además, se considera que se deben crear carreras y especialidades que cubran estas brechas de falta de especialistas en el tema.

El análisis regulatorio en Perú y su potencial impacto en Ecuador

Perú ha logrado establecer un marco legal bastante sólido, constituyéndose en un referente para los demás países latinoamericanos.

Marco normativo peruano

Perú cuenta con un sistema de protección de datos personales que se ha fortalecido en la última década, dentro de este marco normativo, se encuentra lo siguiente:

- Constitución Política del Perú (1993), que en su artículo 2, inciso 6, reconoce el derecho fundamental a la protección de datos personales a través del habeas data.
- Ley N° 29733 de Protección de Datos Personales (2011), que en lo principal, establece el marco general de protección, incluyendo principios rectores, derechos de los titulares y obligaciones de quienes manejan los datos.
- Reglamento de la Ley N° 29733 (2013), esta norma detalla los procedimientos y mecanismos de aplicación de la Ley de Protección de Datos Personales.
- La Autoridad Nacional de Protección de Datos Personales, que es un organismo dependiente del Ministerio de Justicia y Derechos Humanos; y, actúa como el órgano de control especializado en el ramo.
- La Directiva de Seguridad para el tratamiento de Datos Personales, establece las condiciones, requisitos y medidas técnicas que deben aplicarse para cumplir con la Ley N° 29733**,** Ley de Protección de Datos Personales y su reglamento.

Marco jurídico comparado del Perú y su impacto en el Ecuador

Debilidades del Marco Regulatorio en el Perú

Las debilidades en el marco regulatorio de protección de datos personales en Perú pueden impactar significativamente en Ecuador, debido a las estrechas relaciones comerciales, culturales y migratorias que ambos países mantienen. Alvarado (2016), en su artículo ‘La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales’, analiza cómo estas deficiencias podrían influir en el ecosistema de protección de datos en Ecuador, planteando posibles desafíos y oportunidades para mejorar la seguridad y regulación en la región.

Según la documentación revisada, el régimen peruano presenta varias debilidades dentro de las cuales se anotan las siguientes:

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

- No existe una implementación completa del marco normativo; pues, aunque existe la Ley N° 29733 de Protección de Datos Personales y su reglamento, hay una notable discrepancia entre lo que dice la normativa y su aplicación real; lo cual no es únicamente el caso peruano, si no de muchas otras legislaciones.
- La Autoridad Nacional de Protección de Datos, que indica le ley peruana, en la actualidad y debido a la crisis generalizada, enfrenta problemas de presupuesto y falta de personal, lo que afecta su capacidad para actuar y supervisar adecuadamente.
- Existen deficiencias en medidas de seguridad técnicas, sobre todo en las instituciones públicas, la normativa peruana no cuenta con estándares técnicos específicos que se alineen con las amenazas actuales en ciberseguridad, limitándose a requerimientos bastante generales (Seclén Arana, 2016).
- Se vislumbra vacíos normativos en lo que respecta a las transferencias de datos entre países andinos, lo que genera incertidumbre y hasta desconfianza, por el notable valor económico que han adquirido los datos personales (Belli, Nougrères, Mendoza Iserte, Palazzi, & Remolina Angarita, 2023) .
- Tanto en el sector público como en el privado, hay un bajo nivel de conciencia sobre las obligaciones relacionadas con la seguridad de los datos, y sobre el peligro que conlleva al otorgar permisos en plataformas desconocidas.
- El tratamiento transfronterizo sin garantías es un tema que debe abordarse a nivel de Latinoamérica, por ser un tema delicado, pues existe mucha información sensible de los ecuatorianos, relacionada con diversos aspectos, como son salud, finanzas, educación, etc., que en los actuales momentos ya no sólo se procesa en nuestro país, si no que ha trascendido fronteras y no se tiene la garantías que éstos datos sean tratados con las protecciones adecuadas, lo que pone a los titulares en riesgo.
- Además, se tiene la minimización de los estándares de consentimiento, que constituye un problema que no se puede pasar por alto; tanto en Perú como en Ecuador, éste consentimiento se presenta de forma casi imperceptible, y el usuario de plataformas digitales no tiene plena conciencia de los permisos otorgados.
- En lo social, existen brechas de desigualdad digital, por las profundas diferencias entre distintos grupos sociales, que ocasiona que se afecte especialmente a las poblaciones vulnerables que tienen mayor desconocimiento y poca o nula alfabetización digital.

Desafíos específicos para Ecuador

Siendo Perú un país vecino, con un alto tránsito de movilidad, no solo que es necesaria esa transnacionalización de datos, si no que se transforma en una urgencia, por lo tanto, se considera que: primero, se debe procurar la armonización normativa, donde Ecuador debe resistir la presión de reducir sus estándares de protección de datos, para facilitar los intercambios con Perú, y más bien, fijar políticas donde ambos países lleguen a consensos.

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

Con este movimiento migratorio y comercial, la supervisión de los flujos de datos que cruzan fronteras es un desafío constante, la autoridad ecuatoriana necesita encontrar una forma efectiva de monitorear las transferencias de datos hacia los países que cuentan con mecanismos de control más débiles.

La manera en que Ecuador aborde estas cuestiones es crucial, para determinar si sus relaciones digitales con Perú se convierten en una oportunidad para fortalecer su sistema nacional de protección de datos personales o, por el contrario, se transforman en un factor que lo debilite; lo cual, a su vez, tendrá un impacto en los derechos fundamentales de los ciudadanos ecuatorianos en esta, la era digital.

4. CONCLUSIONES

El método de derecho comparado juega un papel clave al permitir identificar las similitudes y diferencias en las legislaciones sobre la seguridad de datos personales en Colombia, Perú, Chile y Ecuador; esto permite entender cómo cada país está abordando los problemas relacionados con la tecnología, la producción y el comercio, así como los conflictos que surgen a nivel internacional, en este contexto, se refuerza la importancia de la colaboración y cooperación entre naciones, siendo esencial crear un sistema coherente que beneficie a todos los actores involucrados, además, de construir alianzas y convenios que busquen minimizar los problemas de seguridad de datos, garantizando así la protección de la información personal de los ciudadanos en los diversos países de la región.

Las falencias detectadas en la normativa de Chile constituyen una alerta para Ecuador, en particular por los nexos sociales, económicos y tecnológicos que existe entre ambos países. Con el fin de reducir estos riesgos, Ecuador podría: Fortalecer su marco regulatorio enfocándose particularmente en las transferencias internacionales, instaurar programas de colaboración técnica con otros países líderes, como Colombia, que han desarrollado sistemas más sólidos, fomentar iniciativas regionales para equilibrar los estándares de protección, previniendo de esta manera un descenso en la región andina, e instaurar sistemas de certificación y auditoría específicos para las compañías chilenas que gestionan y manejan datos sensibles de los ecuatorianos.

Al comparar las legislaciones de Colombia y Ecuador en materia de protección de datos personales, se evidencian diferencias significativas en su enfoque; Colombia ofrece valiosas lecciones que Ecuador podría considerar al desarrollar su propia normativa, es crucial que este proceso tome en cuenta las particularidades sociales, económicas y culturales del país, evitando una simple réplica del modelo colombiano; pues, para garantizar una protección efectiva de los datos personales en Ecuador, se requiere un enfoque integral que combine el desarrollo normativo, la implementación tecnológica y un cambio cultural, este enfoque permitirá la creación de un sistema de protección de datos adaptado a las realidades y necesidades nacionales, contribuyendo a la preservación de los derechos fundamentales de los ciudadanos en la era digital.

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

El estudio comparativo entre Perú y Ecuador muestra diferencias notables en sus perspectivas respecto a la salvaguarda de la información personal; mientras que Perú posee un marco regulatorio más sólido y una mayor experiencia institucional, Ecuador permanece en las primeras fases de puesta en marcha de su ley en este campo, con débiles avances; la experiencia peruana resalta la relevancia de hacerlo de forma gradual, particularmente en contextos caracterizados por desigualdades digitales y diversidad sociocultural. Simultáneamente, el análisis, expone los retos que se presentan cuando hay restricciones institucionales y presupuestarias para construir un sistema de seguridad de datos que se ajuste a la realidad social, cultural y económica; y, que a su vez garantice de manera efectiva los derechos de sus ciudadanos en la era digital.

Para lograr una implementación exitosa de la norma, será necesario no solo establecer líneas de acción, sino también fortalecer las instituciones, adaptar la tecnología, incrementar la investigación y fomentar un cambio cultural, con un compromiso constante que vaya de lo político a lo social; solo así, se asegurará que se consolide una cultura de respeto hacia la privacidad y una gestión responsable de la información personal de los ecuatorianos.

REFERENCIAS

Alvarado, F. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Foro Jurídico*, 26.

Álvarez Valenzuela, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalizacion del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología*, 1-4.

Asamblea Constituyente del Ecuador. (2008). Constitución de la República del Ecuador. *Regstro Oficial del Ecuador*. Quito.

Asamblea Nacional Constituyente. (20 de Julio de 1991). Constitución Política de Colombia. Bogotá, Colombia: Diario Oficial No. 40.545.

Asamblea Nacional del Ecuador. (26 de mayo de 2021). Ley Orgánica de Protección de Datos Personales. *Registro Oficial Suplemento 459*. Quito, Pichincha, Ecuador: Registro Oficial.

Belli, L., Nougrères, A. B., Mendoza Iserte, J., Palazzi, P. A., & Remolina Angarita, N. (2023). *Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales.* Buenos Aires: Centro de Estudios en Tecnología y Sociedad.

Benucci Diaz, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. *Revista chilena de derecho y tecnología*, 227-279.

Campos, M. M., & Mújica, L. A. (2008). El análisis de contenido: Una forma de abordaje metodológico. *Laurus, Revista de educación*, 129-144.

Cerda Silva, A. (2018). Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes. *Revista Chilena de Derecho y Tecnología*, 227-279.

Congreso de la República de Colombia. (31 de Diciembre de 2008). Ley 1266 de 2008. Bogotá: Diario Oficial No. 47.219.

Congreso de la República de Colombia. (17 de octubre de 2012). Ley 1581 de 2012. Bogotá, Colombia: Diario Oficial Nº 48587.

Congreso de la República del Perú. (29 de Diciembre de 1993). Constitución de la República

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

de Perú. Lima, Perú.

Congreso de la República del Perú. (3 de Julio de 2011). Ley N° 29733 Protección de Datos Personales. Lima, Perú: Diario Oficial El Peruano.

Congreso Nacional de Chile. (28 de Agosto de 1999). LEY Nº 19.628, sobre protecciòn de la vida privada. Santiago, Chile: Diario Oficial de la República de Chile.

Contreras Amaro, M. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad (REDS)*, 151-162.

Corte Constitucional de Colombia. (16 de Julio de 1992). *Derecho a la Intimidad Personal y Familiar / Derecho a la Informacioin.* Obtenido de https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Flyvbjerg, B. (2011). Caso de Estudio. *The Sage Handbook of Qualitative Research*, 301-316.

Ministerio de Justicia y Derechos Humanos. (22 de Marzo de 2013). Reglamento de la Ley N° 29733. *Decreto Supremo N° 003-2013-JUS*. Perú: Ministerio de Justicia y Derechos Humanos.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (15 de Agosto de 2019). Guia para tratamiento de datos personales en la administración pública. Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

Morlino, L. (2018). *Comparación. Una introducción metodológica para las ciencias sociales.* Toronto: Barbara Budrich Publishers.

Pérez Luño, A. E. (2017). La protección de datos en España: Presente y Futuro. *Informática y Derecho*, 235-246.

Piovani, J. I., & Krawczyk, N. (2021). Los Estudios Comparativos: Algunas notas hostóricas, epistemiológicas y metodológicas. *Educação & Realidade*, 821-840.

Presidencia de la República de Colombia. (27 de junio de 2013). Decreto Nº 1377 de 2013. Bogotá: Diario Oficial No. 48.834.

Presidencia del Perú. (03 de 07 de 2011). *Ley 29733, Ley de Protección de Datos Personales.* Obtenido de https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Remolina Angarita, N., & Álvarez Zuluaga, L. F. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales: Recomendaciones para los países latinoamericanos.* Bogotá: Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *NOVUMJUS*, 107-139.

Sartori, G. (1994). Comparacion y Método comparativo. En J. Ruzzo, & M. Ruíz de Azúa, *La comparación en las ciencias sociales* (págs. 29-50). Madrid: Alianza Editorial S. A.

Schreier, M. (2012). *Qualitative content analysis in practice.* Londres: SAGE Publications.

Seclén Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas. Lima, Perú: Universidad Mayor de San Marcos.

Superintendencia de Industria y Comercio. (2023). *Manejo de información personal, 'Habeas data.* Obtenido de https://www.sic.gov.co/manejo-de-informacion-personal

Taruffo, M. (2016). Consideraciones sobre el precedente. *IUS ET VERITAS*, 330-342.

Fecha de recepción: 24 / 03 / 2025
Fecha de aceptación: 22 / 04 / 2025
Fecha de publicación: 18 / 07 / 2025

Viollier, P. (2017). *El Estado en la protección de datos personales en Chile.* Santiago de Chile: Derechos Digitales.

Zeigert, K., & Kötz, H. (1987). *Infroducción al Derecho Comparado.* Grand Bretaña: Universidad de Oxford.