Maestría en

Derecho Digital con mención en innovación jurídica y legaltech.

Trabajo de investigación previo a la obtención del título de

Magíster en (Derecho Digital con mención en innovación jurídica y legaltech.)

AUTORES:

AB. ANDREA XIMENA BRITO CONTERO

AB. LUIS ALEJANDRO BAEZ GÓMEZ

AB. WILFRIDO LEONARDO ARREAGA ZAMBRANO

AB. STEFANO NICOLAS VELÁSTEGUI VERDEZOTO

AB. MESIAS ANDRÉS OCHOA CASTILLO

TUTORES:

Docente titulación

Profesor PBL1

Profesor PBL2

Profesor PBL3

LA AUTORIZACION PARA LA COMUNICACIÓN O TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES EN EL ECUADOR

Quito, septiembre de 2025

Certificación de autoría

Nosotros, **Wilfrido Leonardo Arreaga Zambrano, Luis Alejandro Baez Gómez, Andrea Ximena Brito Contero, Mesias Andrés Ochoa Castillo; y, Stefano Nicolas Velástegui Verdezoto,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
WILFRIDO LEONARDO ARREAGA ZAMBRANO
Validar únicamente con FirmaEC

Firma del graduando
Wilfrido Leonardo Arreaga Zambrano

Firmado electrónicamente por:
LUIS ALEJANDRO BAEZ GOMEZ
Validar únicamente con FirmaEC

Firma del graduando
Luis Alejandro Baez Gómez

Firmado electrónicamente por:
ANDREA XIMENA BRITO CONTERO
Validar únicamente con FirmaEC

Firma del graduando
Andrea Ximena Brito Contero

Firmado electrónicamente por:
MESIAS ANDRES OCHOA CASTILLO
Validar únicamente con FirmaEC

Firma del graduando
Mesias Andrés Ochoa Castillo

STEFANO NICOLAS VELASTEGUI VERDEZOTO

Firmado digitalmente por STEFANO NICOLAS VELASTEGUI VERDEZOTO
Fecha: 2026.04.14 15:02:20 -05'00'

Firma del graduando
Stefano Nicolas Velástegui Verdezoto

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Wilfrido Leonardo Arreaga Zambrano, Luis Alejandro Baez Gómez, Andrea Ximena Brito Contero, Mesias Andrés Ochoa Castillo; y, Stefano Nicolas Velástegui Verdezoto,** en calidad de autores del trabajo de investigación titulado ***LA AUTORIZACION PARA LA COMUNICACIÓN O TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES EN EL ECUADOR***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (mes año)

Firmado electrónicamente por:
WILFRIDO LEONARDO ARREAGA ZAMBRANO
Validar únicamente con FirmaEC

Firma del graduando

Wilfrido Leonardo Arreaga Zambrano

Firmado electrónicamente por:
LUIS ALEJANDRO BAEZ GOMEZ
Validar únicamente con FirmaEC

Firma del graduando

Luis Alejandro Baez Gómez

Firmado electrónicamente por:
ANDREA XIMENA BRITO CONTERO
Validar únicamente con FirmaEC

Firma del graduando

Andrea Ximena Brito Contero

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MESIAS ANDRES OCHOA CASTILLO

Firma del graduando

Mesias Andrés Ochoa Castillo

STEFANO NICOLAS VELASTEGUI VERDEZOTO

Firmado digitalmente por STEFANO NICOLAS VELASTEGUI VERDEZOTO
Fecha: 2026.04.15 13:48:41 -05'00'

Firma del graduando

Stefano Nicolas Velástegui Verdezoto

Acuerdo de confidencialidad

La Biblioteca de la Universidad Internacional del Ecuador se compromete a:

1. No divulgar, utilizar ni revelar a otros la **información confidencial** obtenida en el presente trabajo, ya sea intencionalmente o por falta de cuidado en su manejo, en forma personal o bien a través de sus empleados.

2. Manejar la **información confidencial** de la misma manera en que se maneja la información propia de carácter confidencial, la cual bajo ninguna circunstancia podrá estar por debajo de los estándares aceptables de debida diligencia y prudencia.

Coordinador Maestría en
Gestión de riesgos

Gabriela Fernández
Gestora Cultural

Aprobación de dirección y coordinación del programa

Nosotros, **Nombre del Director/a EIG y Coordinador/a UIDE,** declaramos que los graduandos: **Wilfrido Leonardo Arreaga Zambrano, Luis Alejandro Baez Gómez, Andrea Ximena Brito Contero, Mesias Andrés Ochoa Castillo; y, Stefano Nicolas Velástegui Verdezoto** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

_____

Director/a de la

Maestría en _____

Francisco Jose Jativa Yanez

Time Stamping Security Data

_____

Coordinador/a de la

Maestría en _____

DEDICATORIA

Abg.WILFRIDO LEONARDO ARREAGA ZAMBRANO, dedico este nuevo triunfo académico a mis padres Ele y Wilfrido que han sido mi apoyo en todo momento y quienes siempre me han impulsado a mejorar constantemente.

Abg. LUIS ALEJANDRO BÁEZ GÓMEZ, este trabajo está dedicado a mis amados padres, Luis e Isabel. Su apoyo incondicional ha sido la base de todo lo que he logrado; sin él, nada en mi vida habría sido posible. Gracias a su guía y amor, mi vida ha encontrado un verdadero sentido.

Abg. MESIAS ANDRES OCHOA CASTILLO, dedico este trabajo a mi madre quien ha sido la fuente de luz en mi vida, a mi hermano por sus consejos y no dejar que me rinda.

Abg ANDREA XIMENA BRITO CONTERO, quiero agradecer a Dios por ser mi guía, por darme la fortaleza, la valentía y la fe para seguir adelante, por enseñarme que sus tiempos son perfectos, incluso en los momentos difíciles. A mis hijas Anahí y Camila quienes son mi motor e inspiración. Su amor y su paciencia me impulsaron a no rendir y con determinación poder alcanzar este objetivo. Todo este esfuerzo es para ustedes.

Abg. STEFANO NICOLÁS VELÁSTEGUI VERDEZOTO, el presente trabajo lo dedico, en primer lugar, a mis padres, por su apoyo incondicional y constante en cada uno de mis proyectos académicos y profesionales. A mis hermanos, por ser una fuente permanente de inspiración y motivación. Finalmente, a Raquel, por su apoyo, comprensión y fortaleza compartida, especialmente en los momentos más difíciles de este proceso.

AGRADECIMIENTOS

Nuestro profundo agradecimiento a la Universidad Internacional del Ecuador por la excelencia académica ofrecida y por proveernos los recursos necesarios para llevar a cabo esta investigación.
Extiendemos nuestra gratitud al distinguido jurado y a las autoridades por su tiempo y consideración.

RESUMEN

El presente proyecto de titulación aborda la regulación de las transferencias y comunicaciones internacionales de datos personales en el Ecuador, a partir del análisis de las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales (LOPDP).

La promulgación de la LOPDP en el año 2021 constituyó un avance significativo en el ordenamiento jurídico ecuatoriano, al establecer un marco normativo integral para el tratamiento de datos personales tanto en el sector público como en el privado, pese a tomar referencia a las legislaciones internacionales, presenta vacíos normativos, ambigüedades conceptuales y contradicciones internas que dificultan su aplicación efectiva, particularmente en lo referente a la transferencia o comunicación internacional de datos personales.

El problema central que analiza esta investigación se relaciona con la falta de delimitación clara entre las figuras de “transferencia internacional de datos personales” y “comunicación internacional de datos personales”, así como con la ausencia de criterios objetivos y procedimientos definidos para determinar cuándo un país, organización o empresa receptora garantiza un nivel adecuado de protección de datos personales.

El trabajo tiene como objetivo general proponer una reforma a los capítulos V y IX de la LOPDP, orientada a corregir las contradicciones existentes y a fortalecer el régimen jurídico de las transferencias internacionales de datos personales en el Ecuador.

La metodología de la investigación se desarrolla bajo un enfoque cualitativo, de carácter teórico, jurídico y reformador. Se emplea el método de derecho comparado para analizar las similitudes y diferencias entre la normativa ecuatoriana y los principales estándares internacionales en materia de protección de datos personales. Asimismo, se utiliza un método analítico-interpretativo para examinar el contenido de la LOPDP, su reglamento y la jurisprudencia constitucional relevante, especialmente aquella relacionada con el

derecho a la autodeterminación informativa y la naturaleza jurídica del tratamiento de datos personales.

La presente investigación propone una reforma normativa que permita diferenciar con precisión las figuras de transferencia y comunicación internacional de datos personales.

Palabras Claves: Protección de datos personales, Transferencia internacional de datos, Comunicación internacional de datos, Nivel adecuado de protección, Ley Orgánica de Protección de Datos Personales

ABSTRACT

This degree project analyzes the regulation of international transfers and communications of personal data in Ecuador, based on the examination of the provisions established in the Organic Law on Personal Data Protection (LOPDP). The enactment of the LOPDP in 2021 represented a significant step forward in the Ecuadorian legal system by introducing a comprehensive framework for the processing of personal data in both the public and private sectors. However, despite being inspired by international legal models, the law presents regulatory gaps, conceptual ambiguities, and internal inconsistencies that hinder its effective application, particularly with regard to international data transfers and communications.

The central issue addressed in this research lies in the lack of a clear legal distinction between the concepts of “international transfer of personal data” and “international communication of personal data,” as well as in the absence of objective criteria and defined procedures to determine when a receiving country, organization, or company ensures an adequate level of personal data protection.

In this context, the general objective of the study is to propose a reform of Chapters V and IX of the LOPDP, aimed at correcting the identified inconsistencies and strengthening the legal framework governing international personal data transfers in Ecuador.

From a methodological perspective, the research adopts a qualitative approach of a theoretical, legal, and reform-oriented nature. The comparative law method is applied to examine the similarities and differences between Ecuadorian regulations and the main international standards on personal data protection. In addition, an analytical and interpretative method is used to assess the LOPDP, its regulatory framework, and relevant constitutional case law, particularly concerning the right to informational self-determination and the legal nature of personal data processing.

Based on this analysis, the research proposes a normative reform that allows for a clearer differentiation between international data transfer and communication, with the purpose of

enhancing legal certainty and ensuring the effective protection of personal data subjects' rights.

Keywords: Personal data protection, International data transfer, International data communication, Adequate level of protection, Organic Law on Personal Data Protection.

INDICE

INTRODUCCIÓN

Con la necesidad de garantizar y reconocer los derechos a la protección de los datos de carácter personal tal como lo consagra la Constitución de la República del Ecuador en su artículo 66, numeral 19, se creó la Ley Orgánica de Protección de Datos Personales en Ecuador publicada en el registro oficial en mayo del 2021, donde Ecuador dio un paso importante a la tutela de la protección de datos de carácter personal, este derecho permite a su titular decidir sobre sus datos personales dentro del territorio ecuatoriano, así como establece un tratamiento adecuado para una correcta recolección, almacenamiento, distribución y/o difusión de estos, siempre y cuando exista una autorización expresa del titular del derecho protegido.

Esta nueva Ley Orgánica trajo consigo algunas incongruencias dentro de la legislación ecuatoriana, en cómo se definen con las leyes internacionales que abarcan el tema de la transferencia o comunicación internacional de datos personales.

En particular se ha generado una problemática a la hora de interpretar la Ley respecto a la transferencia o comunicación internacional de datos personales, la ley ha establecido que la Autoridad de Control deberá establecer los listados donde consten los países que hayan sido declarados con un nivel adecuado de protección de datos personales de acuerdo a la LOPDP, sin establecer los criterios de cuáles son los niveles adecuados de protección y de la misma forma no se delimita cuando se considerara como transferencia o comunicación internacional de datos personales, por lo que para el presente proyecto de tesis, está enfocado en encontrar la claridad en estos aspectos en los principios de autorización ya establecidos.

1. Antecedentes del tema

El camino hacia la protección de datos personales en Ecuador es una historia de evolución conceptual, que comienza con el derecho a la privacidad y culmina en la autodeterminación informativa, este derecho, que faculta al ciudadano a decidir sobre su propia información, emergió internacionalmente hace décadas, pero en el contexto nacional, su plena aplicación tardó en llegar.

Aunque las Constituciones de 1998 y 2008 reconocieron firmemente el derecho a la protección de datos, anclándolo en la figura del Hábeas Data, esta protección fue, durante mucho tiempo, incompleta, el Hábeas Data funcionó primariamente como una herramienta de reparación post-daño al no existir una ley específica ni una autoridad de control con poderes preventivos, el sistema carecía de la capacidad para gestionar el volumen masivo de datos que circulaban en la nueva era digital, dejando al ciudadano con una defensa reactiva ante un problema que crecía exponencialmente.

La realidad digital no espera, y la falta de un marco legal especializado se convirtió rápidamente en un problema para el Ecuador que se encontraba rezagado, incapaz de alinearse con estándares globales, siendo el Reglamento General de Protección de Datos de la Unión Europea la referencia ineludible.

La promulgación de la Ley Orgánica de Protección de Datos Personales marcó un punto de inflexión, transformando el enfoque de la protección, sin embargo, las contradicciones en el flujo revelaron una fragilidad notable al intentar regular uno de los aspectos más complejos la transferencia y comunicación internacional de datos que emplea los términos "Transferencia" y "Comunicación" de manera indistinta. En la práctica jurídica, esto es inaceptable, ya que una transferencia implica un cambio de responsable y de control,

mientras que una comunicación es solo un acceso por parte de un encargado, esta ambigüedad siembra inseguridad jurídica sobre la responsabilidad del tratamiento.

2. Contextualización del problema en el ámbito jurídico nacional e internacional

El uso excesivo de la tecnología ha generado que se incremente de manera significativa el manejo de los datos personales en la globalización digital en la que nos enfrentamos, sin un debido control del destino exacto que estos tengan al momento de ser comunicados o transferidos a terceros, convirtiéndose en una actividad económica muy lucrativa en la actualidad, escenario que plantea desafíos relevantes frente a un correcto alcance yprotección que se da al manejo de esta información.

Dentro de nuestro ordenamiento jurídico, tanto la Constitución de la República del Ecuador, así como la LOPDP, buscan garantizar una correcta regulación y una debida protección en especial al momento de que estos datos personales sean comunicados o transferidos a un tercero, determinando que exista niveles adecuados de protección a los países o terceros que manejaran la información, pero al momento de interpretarla se evidencian contradicciones y ambigüedades que dificultan su correcta implementación.

Estas contradicciones se han reflejado en poder determinar de manera clara y correcta el alcance que tienen estas comunicaciones así como las transferencias internacionales, ya que no determinan el alcance y por ende las responsabilidades de los diferentes actores que intervienen dentro de la protección de los datos personales, el no poder distinguir los diferentes los tipos comunicaciones que se pueden presentar y no contar con parámetros establecidos genera inseguridad jurídica para los responsables, los encargados del tratamiento como para los titulares de los datos personales.

En el ámbito internacional, se puede evidenciar que las transferencias internacionales de datos personales se encuentran direccionadas porestándares sólidos, como el Reglamento General de Protección de Datos de la Unión Europea (RGPD), ylas directrices de la OCDE siendo las más relevantes. Normativa y directrices que han permitido generar criterios uniformes, con responsabilidad proactiva y garantías para los diferentes actores

de la protección de datos personales, lo cual no se ajusta a lo determinado en la normativa ecuatoriana.

Con lo expuesto, podemos determinar que el problema jurídico se centra en la falta de claridad de conceptos y el alcance que se debe dar a la comunicaciones y las transferencias de los datos personales, ya que no permite delimitar correctamente las responsabilidades que los diferentes actores del tratamiento que permita contar con garantías de una debida protección, lo que puede derivar en una protección insuficiente de los derechos de los titulares, De ahí radica la necesidad de analizar y proponer un reforma a los capítulos V y IX, que permitan una correcta interpretación y aplicación de la LOPDP en relación con los estándares internacionales de protección de datos personales.

3. Planteamiento del problema

El presente proyecto tiene como propósito analizar las contradicciones de las transferencias o comunicaciones internacionales de Datos Personales en el Ecuador, generando parámetros para cada caso, mismo que está regulado en la Ley Orgánica de Protección de Datos Personales (LOPDP); y proponer una reforma a los capítulos V y IX en los artículos que aplican para su ejecución, todo esto tomando en consideración el Reglamento de la Ley De Protección de Datos Personales de la Unión Europea, entre otras legislaciones en materia de transferencia o comunicación internacional de datos personales. Es decir, delimitar o distinguir cuando se usara la figura de “transferencia internacional de datos personales” y “comunicación internacional de datos personales”.

Una vez determinados los parámetros para las transferencias o comunicaciones de datos personales, definir el proceso para que la Autoridad de Control establezca de manera clara y precisa, que países o empresas cuentan con niveles adecuados para la transferencia o comunicación internacional de datos personales.

4. Formulación de la pregunta de investigación

¿Cómo debe reformarse la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador, específicamente en sus capítulos V y IX, para corregir las contradicciones existentes en los lineamientos de autorización aplicables a la transferencia y comunicación internacional de datos personales, delimitando con seguridad jurídica sus conceptos y supuestos, a partir de un análisis comparado con el RGPD (Unión Europea) y el Marco de Privacidad de Datos UE–EE. UU. (DPF), qué factores y procedimiento metodológico debería adoptar la Autoridad de Control para evaluar y determinar el "nivel adecuado de protección" de países y empresas receptoras?

5. Justificación de la investigación

La presente investigación se centra en la autorización para la comunicación o transferencias internacionales de datos personales dentro del marco de la Ley Orgánica de Protección de Datos Personales de Ecuador, para lo cual, se aborda una problemática de gran relevancia en la era de la comunicación digital y el tratamiento de los datos personales. En este sentido el presente trabajo se centra en los alcances legales, teóricos y prácticos.

La Ley Orgánica de Protección de Datos Personales, aunque moderna, presenta vacíos en sus Capítulos V y IX en lo que respecta a la regulación de las transferencias o comunicación internacionales de datos personales, que sea clara y que permita fortalecer una seguridad jurídica tanto para la Autoridad de Control como para los responsables del tratamiento de datos personales. La ambigüedad existente en la figura de transferencia o comunicación internacional de datos y del proceso para determinar un nivel adecuado para su protección, genera un riesgo latente de interpretaciones contradictorias, lo cual vulnera la certeza del marco legal, incrementando el riesgo de incumplimientos, ya que no se delimita cuando se considerara como transferencia internacional de datos personales o comunicación internacional de datos personales.

En la actualidad, la globalización y la digitalización de la información han hecho que el flujo transfronterizo de datos sea una práctica cotidiana e indispensable para el funcionamiento del comercio, la educación, la salud y los servicios digitales. Este contexto exige que los marcos jurídicos nacionales se adecuen a estándares internacionales, garantizando tanto la seguridad jurídica de las organizaciones que manejan datos, como la efectiva protección de los derechos de los titulares. Sin embargo, la LOPDP carece de criterios claros sobre qué debe entenderse por un “nivel adecuado de protección” y no establece los parámetros técnicos ni jurídicos que deben guiar a la Autoridad de Control al momento de autorizar dichas transferencias.

Desde esta perspectiva, este trabajo contribuye a la doctrina legal ecuatoriana al realizar un análisis explicativo de la normativa nacional a la luz de referentes internacionales que son mucho más fiables y robustos.

El realizar un análisis comparativo de la normativa legal ecuatoriano con el Reglamento General de Protección de Datos de la Unión Europea y el Marco de Privacidad de Datos de Estados Unidos permitirá tener una visión más amplia de la problemática y establecer bases conceptuales más sólidas para una correcta regulación legal, la cual sea a su vez más armónica, moderna y alineada con los estándares de derechos humanos de cuarta generación y con los conceptos internacionales.

El estudio se justifica además por su valor propositivo y de aporte jurídico, ya que no solo pretende identificar y analizar las contradicciones existentes, sino también proponer parámetros normativos claros y coherentes que orienten la actuación de la Autoridad de Control y de los responsables del tratamiento. La comparación con marcos consolidados como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y el Marco de Privacidad de Datos UE-EE. UU. (Data Privacy Framework) permitirá establecer

un punto de referencia internacional que oriente la adecuación de la legislación ecuatoriana a los estándares globales de protección.

Por otra parte, este trabajo ofrece una solución concreta para la Autoridad de Control, al delimitar los parámetros objetivos que deben utilizarse para evaluar y emitir la autorización para la transferencia o comunicación internacional de datos personales. Esto optimiza la gestión regulatoria y asegura la tutela efectiva del derecho.

En su dimensión social, el presente trabajo tiene como fin último el garantizar que los derechos de los titulares de datos personales no se vean vulnerados al momento de realizarse una transferencia o comunicación internacional de datos personales de los mismos, proponiendo estándares basados en la normativa internacional aseguramos que esta protección sea transfronteriza.

Por lo expuesto, el presente trabajo al establecer una propuesta de reforma ofrece mecanismos claros y previsibles que facilitarán la transferencia internacional de datos, evitando la paralización de flujos de datos esenciales bajo un marco de cumplimiento sólido.

6. Objetivos: general y específicos

OBJETIVO GENERAL:

Proponer una reforma a las contradicciones existentes en los lineamientos determinados de transferencias o comunicaciones internacionales de datos personales en el Ecuador, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP).

OBJETIVO ESPECIFICO:

- Identificar las contradicciones de las disposiciones de la LOPDP en lo referente a las transferencias o comunicaciones internacionales de datos personales,

especialmente los capítulos V y IX, con el REGLAMENTO GENERAL DE PROTECCION DE DATOS de la Unión Europea.

- Elaborar un cuadro comparativo entre la LOPDP, el RGPD (UE) y el Marco de Privacidad de Datos UE-EE. UU. (DPF), determinando las buenas prácticas y los criterios técnicos y jurídicos trasladables para garantizar un nivel adecuado de protección en Ecuador.
- Redactar una propuesta articulada de reforma para los Capítulos V y IX de la LOPDP que delimite, con seguridad jurídica, los conceptos y supuestos de transferencia y la Comunicación internacional de datos personales.
- Desarrollar una guía de factores y un procedimiento metodológico para que la Autoridad de Control evalúe y determine el Nivel Adecuado de Protección de países y empresas receptoras, optimizando el proceso de autorización.

7. Metodología de investigación

El presente trabajo de titulación se enmarca en un proyecto de investigación jurídica tipo cualitativo, teórico y reformador, se usará método de derecho comparado, orientado al análisis a la ley y se hará una propuesta de reforma a una problemática identificada, se empleará los siguientes métodos de investigación:

- Método Cualitativo: Se analizará el contenido y alcance de las normas pertinentes de la LOPDP como lo son los artículos contenidos en los capítulos V y IX, interpretándolas de manera sistemática dentro del ordenamiento jurídico ecuatoriano, las normas vigentes y leyes internacionales; esto en lo referente a la comunicación y trasferencia internacional de datos personales.

- Método de Derecho Comparado: Se recurrirá a otros ordenamientos jurídicos internacionales, como el Reglamento General de Protección de Datos de la Unión

Europea (GDPR), Marco de privacidad de Datos UE-EEUU (Data privacy framework) para identificar buenas prácticas y soluciones que puedan informar la propuesta de reglamentación para el Ecuador.

- Método Reformador: Se reformará la normativa ecuatoriana vigente, su eficiencia y aplicabilidad de la Ley Orgánica de Protección de Datos Personales, respecto a la autorización para la transferencia o comunicación internacional de datos personales, establecida en los capítulos V y IX, que definirá de manera correcta la aplicación de la transferencia o comunicación internacional de datos personales realizando una diferenciación a esta figura.

CAPÍTULO I. MARCO TEÓRICO Y CONCEPTUAL DE LA PROTECCIÓN DE DATOS PERSONALES, TRANSFERENCIA Y COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES EN EL DERECHO ECUATORIANO

1. Concepto y evolución histórica del derecho a la protección de datos personales.

El dato personal se define como la información sea en formato físico o digital, en los cuales puede constar, nombres, apellidos, direcciones, cuentas bancarias, información laboral, de salud o cualquier otro tipo de información que debe ser considerada de carácter privado o reservado de cada persona.

Esta información para ser almacenada o tratada debe contar con una autorización estrictamente expresa de su titular, sin esta autorización, no se puede acceder a estos datos y aun cuando se cuente con la autorización de su titular esta información debe ser previamente tratada y especificarse que uso y alcance se le dará.

En la actualidad, esta información es almacenada en sistemas informáticos, bases de datos, nubes entre otros tipos de almacenamientos masivos, los cuales están conectados a internet. Esta huella digital es regulada por la Unión Europea mediante el REGLAMENTO GENERAL DE DATOS PERSONALES, y en Ecuador mediante la LEY ORGANICA GENERAL DE DATOS PERSONALES y EL REGLAMENTO ORGANICO GENERAL DE DATOS PERSONALES.

2. Fundamento constitucional del derecho a la protección de datos personales en el Ecuador

El estado ecuatoriano en su Constitución de la República del Ecuador del 2008 establece que garantiza los principios de intimidad, privacidad, los cuales se pueden considerar como pilares para garantizar el derecho a la protección de datos personales, tal es así que

el artículo 66 numeral 19 de la Constitución de la República del Ecuador se establece el derecho a la protección de datos personales.

“Art. 66.- Se reconoce y garantizará a las personas: … 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.”, el estado garantiza la protección de datos personales de cada persona natural, esto en concordancia con el derecho a la intimidad y la privacidad, pero el titular de los datos personales tiene esa potestad de autorizar el uso de sus datos personales, para que estos sean recolectados, procesados, distribuidos o difundidos, pero a su vez debe ser protegidos pese a dicha autorización del titular de los datos, sea mediante tratamiento de los datos personales, evitando así que estos datos sean difundidos o usados de forma ilegítima y no consentida pese a existir un consentimiento expreso de su titular.

El derecho a la protección de datos se rige por varios principios constitucionales que tienden a ser concordantes con el artículo 66 numeral 19 de La Constitución de la República del Ecuador: 1) principio de autodeterminación informativa y privacidad, todo acto de autorización por parte del titular tiene cierto alcance y es que debe especificarse o informarse para que se usaran dichos datos personales pese a su autorización y así mismo su titular tiene la particularidad de que en cualquier momento negar o revocar dicha autorización; 2) principio de privacidad e intimidad, pese a otorgarse la autorización de los datos personales, estos deben ser tratados, almacenados y recolectados, lo cuales no deben ser susceptible de cualquier vulneración y menos de su difusión o publicación no consentida; 3) principio de consentimiento legalidad, este principio es fundamental ya que ningún dato personal no se debe tratar sin permiso ni consentimiento de su titular y así mismo debe existir el formalismo legal como es el consentimiento del titular de los datos personales; 4) principio de la finalidad y proporcionalidad, es decir que debe indicarse

cuál será la finalidad para la cual se autoriza el uso y tratamiento de los datos personales previa autorización de su titular y especificarse para que casos, y respecto a proporcionalidad es que en el mismo acto de consentimiento para el uso y tratamiento de los datos personales su titular debe conocer que datos son los que permitirán sean usados esto en conjunto con el principio de finalidad de la misma.; y, 5) principio de responsabilidad, si bien este principio no está literalmente redactado en nuestra constitución, el estado tiene éste deber y es el encargado de ser responsable de forma implícita sobre la protección de los datos personales de cada titular.

3. Conceptos clave de la Ley Orgánica de Protección de Datos Personales (LOPDP)

3.1. Datos personales, tratamiento, responsable y encargado

La Ley Orgánica de Protección de Datos Personales (LOPDP) define los datos personales como toda información que identifica o puede identificar a una persona natural, de manera directa o indirecta. Esto incluye nombres, números de cédula, direcciones, datos biométricos, información genética, de salud, laboral o patrimonial, entre otros (art. 4, num. 1, LOPDP, 2021).

El tratamiento de datos personales comprende cualquier operación que se realice sobre esos datos, esto puede ser su recolección, almacenamiento, uso, comunicación o eliminación, ya sea en medios físicos o digitales. Este tratamiento debe realizarse respetando principios como la licitud, transparencia, finalidad y seguridad (art. 4, num. 17 y 5, LOPDP, 2021).

El responsable del tratamiento es la persona natural o jurídica, pública o privada, que decide para qué y cómo se manejarán los datos personales (art. 4, num. 22, LOPDP, 2021). Por otro lado, el encargado del tratamiento es quien realiza operaciones sobre los datos siguiendo las instrucciones del responsable, sin decidir por sí mismo la finalidad o el uso de la información (art. 4, num. 11, LOPDP, 2021). Tanto el responsable como el encargado deben aplicar medidas técnicas y de seguridad adecuadas para evitar accesos

no autorizados, pérdidas o alteraciones de los datos y garantizar los derechos de las personas sobre su información.

3.2. Consentimiento y derechos del titular

El consentimiento del titular es uno de los pilares esenciales para el tratamiento legítimo de los datos personales. Según la LOPDP la persona debe autorizar el uso de sus datos de manera voluntaria, luego de haber recibido información clara sobre el propósito del tratamiento, el tiempo de conservación, las posibles transferencias y los destinatarios de los datos. Además, el titular puede retirar su consentimiento en cualquier momento, sin que esto afecte el tratamiento realizado con anterioridad (arts. 7 y 8, LOPDP, 2021).

Como señala Eduardo Bertoni (2018), el consentimiento informado constituye una expresión concreta del principio de autodeterminación informativa, pues permite que las personas conserven el control sobre su información personal y decidan de manera consciente cómo se utiliza. Este enfoque resalta que la protección de datos no solo es una cuestión técnica o jurídica, sino un derecho fundamental vinculado a la dignidad humana.

La ley también reconoce varios derechos que garantizan el control del titular sobre su información personal, conocidos como derechos ARCO-P, los cuales se encuentran enmarcados en la LOPDP desde el artículo 11 hasta el artículo 16 y son los siguientes:

- Derecho de acceso: permite conocer qué datos se están tratando, su origen, finalidad y quiénes los manejan.
- Derecho de rectificación y actualización: faculta al titular a solicitar la corrección de datos incorrectos o desactualizados.
- Derecho de eliminación o supresión: permite exigir que los datos sean eliminados cuando ya no sean necesarios o cuando se haya revocado el consentimiento.
- Derecho a la oposición: posibilita oponerse al tratamiento por motivos legítimos.
- Derecho a la portabilidad: permite recibir los propios datos en un formato estructurado y transferirlos a otro responsable.

- Derecho a la suspensión del tratamiento: en ciertos casos, el titular puede solicitar la suspensión temporal del tratamiento de sus datos.

4. Principios rectores de la protección de datos personales según la LOPDP

Los principios rectores constituyen la matriz de la LOPDP, ya que orientan la interpretación, aplicación y cumplimiento de todas las disposiciones relacionadas con el tratamiento de la información personal. Su observancia es obligatoria para todas las entidades que manejen datos personales, tanto públicas como privadas.

José Luis Piñar nos señala que los principios de protección de datos representan el fundamento ético y jurídico del derecho a la privacidad, pues garantizan que el tratamiento de la información se realice con respeto a la dignidad humana y a la autonomía de las personas. Son valores esenciales que guían la actuación de quienes gestionan información personal. Entre los principales principios establecidos en la LOPDP se destacan los siguientes, lo cuales están establecidos en el artículo 5 de la ley:

1. **Principio de licitud:** todo tratamiento de datos debe realizarse conforme a la ley y basarse en una causa legítima, como el consentimiento del titular o un mandato legal.
2. **Principio de lealtad y transparencia:** implica que el tratamiento debe ser claro, accesible y honesto, informando al titular sobre la finalidad, el uso de sus datos y los derechos que le asisten.
3. **Principio de finalidad:** los datos personales deben recolectarse con objetivos determinados y legítimos, y no pueden ser usados con propósitos distintos a los informados inicialmente.
4. **Principio de minimización de datos:** solo deben recopilarse los datos estrictamente necesarios para cumplir con la finalidad declarada, evitando el tratamiento excesivo o innecesario.

5. **Principio de exactitud y actualización:** los datos personales deben ser correctos, completos y mantenerse actualizados, adoptando medidas que garanticen su veracidad.
6. **Principio de limitación del plazo de conservación:** los datos deben conservarse solo durante el tiempo necesario para cumplir con la finalidad establecida, luego de lo cual deben eliminarse o anonimizarse.
7. **Principio de integridad y confidencialidad:** exige aplicar medidas de seguridad adecuadas para proteger los datos frente a accesos no autorizados, pérdida o alteración, manteniendo la confidencialidad incluso después de finalizada la relación laboral o contractual.
8. **Principio de responsabilidad proactiva:** obliga a los responsables del tratamiento a demostrar que cumplen efectivamente con las obligaciones legales, implementando políticas internas, auditorías, protocolos de seguridad y mecanismos de control.

Estos principios garantizan que el tratamiento de los datos personales se realice dentro de un marco de respeto a la dignidad, la autodeterminación informativa y la privacidad, pilares fundamentales de una sociedad democrática y digitalmente responsable.

5. Naturaleza jurídica del tratamiento de datos y su relación con los derechos fundamentales.

Realizar un análisis jurídico respecto al tratamiento de datos personales en el ordenamiento legal ecuatoriano, requiere comprender su origen en la Constitución y su regulación posterior dentro de la Ley Orgánica de Protección de Datos Personales.

El tratamiento de datos personales no es la capacidad de cualquier persona para obtener o ejecutar operaciones sobre datos personales de forma ilimitada. Es una facultad jurídica que se encuentra condicionada a las bases de legitimación y principios legales que nacen de la potestad reguladora de la Ley.

Si bien es cierto dentro de la Constitución del Ecuador del 2008, ya presento un artículo que mencionaba el uso de los datos personales y reconocía el derecho de las personas a tener acceso y decisión sobre su información, no fue sino con la promulgación de la Ley Orgánica de Protección de Datos Personales, que se dio inicio a su regulación, lo cual transformo el enfoque de la situación legal del país, es así, que antes de la emisión de la LOPDP, la Constitución del Ecuador en el numeral 19 del artículo 66 únicamente reconoció:

“Art. 66.- Se reconoce y garantizará a las personas: (…)

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.”

El Hábeas Data fue la primera figura legal contemplada, con la finalidad de garantizar el derecho reconocido en la Constitución, estableciendo un esquema remedial donde la intervención legal ocurría tras la vulneración del derecho.

Es por ello que, debemos comprender que la Ley Orgánica de Protección de Datos Personales adopta un marco más proactivo al establecer principios rigurosos que obligan a los responsables y encargados del tratamiento a justificar su actividad de forma preventiva, redefiniendo así la calidad jurídica del tratamiento de datos como un acto de cumplimiento permanente.

La Ley Orgánica de Protección de Datos Personales se basa en el concepto de "Tratamiento" entendiéndose como tal a cualquier operación o conjunto de operaciones realizadas sobre datos personales. Esta definición es amplia e incluye, la recolección, el registro, la organización, la estructuración, el almacenamiento, la recuperación, la consulta, el uso, la divulgación por transmisión, la difusión, la restricción, la eliminación o la destrucción.

Artículo 4 LOPDP.

“Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.”

Este tratamiento, paso de constituir un mera actividad técnica o administrativa, a una actividad jurídica cuyo alcance está regulado por las disposiciones de la Ley Orgánica de Protección de Datos Personales y su Reglamento General, esto amplio el horizonte de los datos personales entendiéndose como tal que al ser parte del individuo su transgresión viola también derechos humanos fundamentales como son el derecho a la intimidad y la privacidad.

Los principios que rigen la protección de datos personales no son discrecionales para quien tiene acceso o hace uso de los mismos, sino que se encuentran bajo regulatorias que definen la legalidad de su tratamiento, limitando así el ejercicio discrecional del responsable. La violación de un principio implica la ilegitimidad de su tratamiento. Es por ello que, la normativa legal del Ecuador exige el cumplimiento de los principios de legalidad, proporcionalidad y necesidad como criterios mínimos y obligatorios para toda operación que involucre la recolección y tratamiento de datos.

El principio de proporcionalidad respecto al tratamiento de datos personales condiciona la naturaleza jurídica del mismo al exigir que el tratamiento sea adecuado, necesario, oportuno, relevante y no excesivo en relación con las finalidades para las cuales fueron recogidos.

Por otra parte, el principio de finalidad implica que, para que una operación de tratamiento sea lícita, su propósito debe estar previamente definido y limitado, por lo cual debe ser determinado, explícito y legítimo para un fin específico, de esta manera se protege a las personas de que sus datos sean utilizados en forma desleal o que se sean utilizados para fines distintos a los cuales fueron recolectados, garantizando que el titular de los datos tenga la plena seguridad de que su información está siendo utilizada con propósitos legales; sin embargo, esta legalidad no es suficiente ya que se debe limitar la obtención de los datos exclusivamente a los necesarios.

La implicación que conlleva la no desproporción en el tratamiento de datos personales implica que incluso si el tratamiento cuenta con base legal válida, los datos recolectados no pueden sobrepasar los estrictamente necesarios para cumplir su propósito legítimo.

Es así como los principios de necesidad y proporcionalidad actúan como filtros, asegurando que la gestión de datos sea un medio restrictivo, haciendo que el responsable del tratamiento de datos sea quien deba probar el cumplimiento de la normativa y la necesidad de cada dato recabado y procesado.

Desde esta perspectiva, y siguiendo las exigencias establecidas en el Reglamento General de Protección de Datos de la Unión Europea, podemos decir que la naturaleza jurídica del tratamiento de datos personales se sustenta en la necesidad de contar con una base de legitimación clara, sin la cual cualquier tipo de tratamiento resultaría ilícito.

Dentro de la Ley Orgánica de Protección de Datos Personales, específicamente en el artículo 7 se identifican al menos siete bases de legitimación, siendo las más comunes:

1. Debe contarse con el consentimiento del titular.

   El titular de los datos debe otorgar su permiso de manera libre, informada, específica e inequívoca para que sus datos sean procesados con una finalidad determinada. El titular tiene el derecho de revocar este consentimiento en cualquier momento.

2. El tratamiento se da en base a un mandato legal o por disposición judicial.

   El tratamiento es necesario y obligatorio cuando una ley expresa impone al responsable la necesidad de tratar los datos, por ejemplo, reportar información fiscal, o cuando existe una orden judicial que así lo exige.

3. En necesario conocer los datos para la elaboración de documentos, como en las fases precontractuales.

   El tratamiento es indispensable para ejecutar un contrato que ya existe con el titular, o para la aplicación de medidas precontractuales solicitadas por el titular como la elaboración de un presupuesto o un borrador de acuerdo.

4. Cuando el tratamiento de datos está ligado directamente a una misión de interés público o al ejercicio de sus potestades como en las disposiciones de la Ley Orgánica de Transparencia y Acceso a la información Publica

5. Cuando es necesario para proteger la vida o salud del titular o de otras personas.

   Por ejemplo, compartir datos médicos urgentes en una emergencia.

6. Cuando existe interés legítimo del responsable o un tercero, siempre que este no prevalezca sobre los derechos y libertades fundamentales del titular.

   Por ejemplo, prevenir el fraude en transacciones bancarias, para lo cual los bancos implementan medidas de seguridad que proporcionan alertas sobre posibles transacciones irregulares, este interés legítimo prevalece sobre el derecho a la intimidad de la persona.

7. Precautelar el uso de datos que constan en bases de datos de acceso público.

   El tratamiento es lícito cuando la información ya ha sido recogida de bases de datos que son manifiestamente públicas como los registros o bases abiertas que publican todas las instituciones públicas en el Portal de Transparencia de la Defensoría del

Pueblo en cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública.

Respecto al consentimiento del titular, debemos considerar que el mismo debe garantizar el control sobre sus datos, para que el consentimiento sea válido debe ser:

1. Libre. - Otorgado sin coacción.
2. Específico. - Relacionado con una finalidad determinada.
3. Inequívoco. - Claro y sin ambigüedades.
4. Informado. - El titular debe ser plenamente consciente de los detalles del tratamiento, incluyendo las finalidades y las posibilidades de revocarlo.

Si el consentimiento carece de uno de estos requisitos da como resultado un tratamiento ilegítimo, es así que se puede establecer que el consentimiento claramente es una manifestación de la autonomía del titular frente a la capacidad de procesamiento del responsable.

5.1. Relación con los derechos Fundamentales

En necesario tener claro que, el derecho a la protección de datos personales, así como su conexión funcional se encuentre relacionado directamente con los derechos a la intimidad, la imagen y el buen nombre de las personas.

La Corte Constitucional del Ecuador en la sentencia 2064-14-EP/21 ha sido clara al establecer que el derecho a la protección de datos personales y la autodeterminación informativa es independiente de otros derechos como la intimidad, la imagen, la honra y el libre desarrollo de la personalidad, aunque guarden conexión bajo ciertos escenarios.[1]

[1] Corte Constitucional del Ecuador. (2021). *Sentencia No. 2064-14-EP/21* (Caso No. 2064-14-EP). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWIkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

En este sentido el derecho a la autodeterminación informativa consiste en la protección de todos aquellos datos que identifican a una persona o la hacen identificable, lo cual confiere al titular el poder de decidir qué información compartir sobre su vida privada y bajo qué lineamientos.

Por otra parte, la Corte Constitucional determino que los datos personales deben ser entendidos de una forma más amplia al indicar en el párrafo 75 y siguientes de la mencionada sentencia lo siguiente:

“En relación a la definición de datos personales, en la antedicha sentencia, esta Corte Constitucional se pronunció de la siguiente manera: Esta Corte considera que los “datos personales e información sobre una persona”, tal como se encuentran recogidos en nuestra Constitución y en función de una interpretación conforme al principio pro homine, deben ser entendidos en su forma más amplia, en el sentido de toda información que haga referencia de forma directa o indirecta a cualquier aspecto relativo a una persona o sus bienes, en sus distintas esferas o dimensiones; susceptible de ser exigida a través de la garantía de hábeas data. Así se advierte que basta que la información –más allá de la forma en que esté contenida– incluya o comunique un aspecto de la persona –objetivo o subjetivo–; o guarde relación con ella, en función de su contenido, finalidad o resultado, para ser considerada como “dato personal” (énfasis añadido).

Por otro lado, el Consejo Europeo de Protección de Datos de la Unión Europea (CEPD) ha definido al concepto de datos personales como: Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

De lo anterior, entonces, se puede desprender que el concepto de 'dato personal' y, por lo tanto, el objeto de protección de la garantía jurisdiccional de hábeas data, es amplio ya que comprende cualquier tipo de dato que atañe a una persona, identificándola o, en su defecto, haciéndola identificable. En segundo lugar, es preciso indicar que el marco de protección de un dato personal es independiente al medio en donde esté contenido aquel; es decir, ya sea que el dato esté materializado, al estar contenido en un medio físico o, inclusive, desmaterializado, como en los casos en los que el dato se encuentre contenido en un medio digital, el ámbito de protección debe ser el mismo en estas dos circunstancias. Ello, sin perjuicio de que el juez, a la hora de resolver sobre esta garantía, tenga el deber de adoptar mecanismos eficaces para la protección de los datos personales; es decir, que considere el medio donde está contenido el dato y las implicaciones de ello."[2]

La Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador constituyó un hito crucial que define el límite jurídico del tratamiento de datos, incluso entre particulares, considerando que la Corte Constitucional analizo una acción de Hábeas Data, la cual fue presentada por una persona para lograr la eliminación de fotografías íntimas y personales que estaban en posesión y tratamiento no autorizado por otra persona natural.

En este sentido, la justicia ecuatoriana no solo determinó que estas fotografías íntimas y personales eran datos personales, sino que además los considero sensibles, esta decisión declaro la vulneración al derecho a la protección de datos personales, considerando que se realizó un tratamiento no autorizado de datos, estableciendo dos puntos fundamentales:

1. El tratamiento de datos es una actividad regulada constitucionalmente, aplicable erga omnes. Por lo cual incluso los particulares están sujetos a la

[2] Corte Constitucional del Ecuador. (2021). *Sentencia No. 2064-14-EP/21* (Caso No. 2064-14-EP). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

obligación de contar con una base de legitimación si su actividad de procesamiento sobrepasa el ámbito privado personal.

2. El momento en que el tratamiento se proyecta fuera del círculo puramente doméstico, adquiere una cualidad jurídica diferente ya que al rebasar la esfera personal se convierte en una actividad que requiere legitimación legal, reforzando la naturaleza del tratamiento como una potestad inherentemente regulada.

Esta sentencia evidenció que, el tratamiento de datos no autorizado vulnera el derecho a la imagen, la honra, el buen nombre y la intimidad. Aunque el derecho a la protección de datos es autónomo, su vulneración mediante el tratamiento ilegítimo suele ser el mecanismo por el cual se afecta la dignidad humana.

Por otra parte, si nos referimos a la trasferencia internacional de datos, debemos considerar que su naturaleza deriva directamente de su tratamiento el cual debe extenderse de manera internacional considerando que el derecho a la protección de datos es fundamental y su seguridad no puede verse menoscabada simplemente porque el tratamiento cruza una frontera determinada, es así que debemos entender que la transferencia internacional consiste en un tratamiento a través del cual el responsable de datos personales ecuatoriano, transfiere hacia un destinatario extranjero los datos, por lo tanto, esta actividad está sujeta a los principios rectores de la Ley Orgánica de Protección de Datos Personales especialmente a los de legalidad, proporcionalidad y necesidad.

6. Rol de la Autoridad de Protección de Datos Personales en Ecuador

La importancia que en el Ecuador se implemente la Ley Orgánica de Protección de Datos Personales, radicó en la evolución que ha tenido el internet en los últimos años y la ausencia de regulaciones especificas en la materia que provocaba abusos constantes de ciertos sectores sobre el manejo indiscriminado de la información, esta implementación ha buscado generar lineamientos claros que permitan una correcta aplicación y por ende

una protección adecuada por cada integrante del sistema de protección de datos personales.

Dentro de los integrantes que contemplan la protección de Datos Personas, se encuentra la Autoridad de Protección de Datos Personas, siendo una entidad independiente, autónoma e imparcial, creada y definida por la LOPDP, con el propósito de garantizar y controlar una correcta a protección de los Datos Personales en el Ecuador, así como de ser el caso establecer e imponer sanciones específicas, con roles definidos desde la prevención, el control, la supervisión, la investigación y la sanción, cuya función principal es velar porque el tratamiento de los Datos Personales se lo realice de manera responsable, lícita, segura en donde se genere un equilibrio entre el uso que se le dé a toda la información, así como se garantice los derechos y libertades de los titulares.

Su ámbito de aplicación incluye a entidades públicas como privadas y de la misma para su gestión goza de autonomía administrativa, técnica, operativa y financiera.

- En su rol de prevención podemos indicar que la Autoridad de Protección de Datos Personales busca anticipar posibles vulneraciones generando un resguardo desde el marco normativo, es decir que se adopten todas las medidas técnicas, organizadas, legales y que su implementación abarque para todos los integrantes del sistema de protección de datos.

- En su rol de control podemos indicar este se encuentra entrelazado con el rol de supervisión e investigación, ya que la facultad que le atribuye esta determinada en validar que exista una correcta aplicación de la LOPDP su reglamento y demás normativa referente a la materia y eso permita un cumplimiento adecuado de todas las responsabilidades y obligaciones inherentes a cada integrante de manera conjunta.

- En su rol sancionador podemos indicar que la Autoridad de Protección de Datos Personales, si bien busca prevenir y controlar una correcta aplicación de la LOPDP, su reglamento y demás normativa referente a la materia, en los casos que correspondan de incumplimiento tiene la potestad de dictar medidas correctivas, así como de imponer sanciones administrativas leves, graves, o muy graves, así como establecer y adoptar medidas de protección.

Contar con una Entidad independiente permite evidenciar una seguridad jurídica para todos los integrantes del sistema de protección de datos personales, ya que existen directrices, lineamientos y resoluciones que proporcionan cierta claridad en cómo deben ser tratados los datos personales, buscando reducir los riesgos legales, dentro de los procesos de implementación, así mismo juega un papel fundamental para la garantía del derecho a la privacidad y al correcto tratamiento de los datos personales en todo el ámbito digital.

7. Marco normativo ecuatoriano sobre transferencias internacionales.

La Ley Orgánica de protección de datos Personal (LOPDP) de ecuador, entro en vigencia desde el mes de mayo del año 2021, esta normativa relata la juridicidad sobre os derechos fundamentales que recaen sobre la protección de datos personales, misma que se encuentra establecida en el artículo 66 numeral 19, de la constitución de la república del Ecuador. Esta tiene por objetivo regular el tratamiento de datos personales tanto en el sector público como en el privado, delimitando los principios de licitud, lealtad, transparencia, minimización, seguridad y responsabilidad proactiva, teniendo como finalidad que el uso que se la a los datos se lo realice respetando el derecho de las personas sobre sus datos y la privacidad de estos.

En lo concerniente a las transferencias de datos personales internacionales, la LOPDP menciona en su artículo 44 estas podrán direccionarse solamente a países u organizaciones que dispongan o tengan el nivel requerido de seguridad en la protección

de datos, este nivel de seguridad será el requerido por la autoridad de Protección de datos personales del Ecuador. Esto se lo realiza obedeciendo el principio de equivalencia normativa, el cual hace referencia a que un país cumple con los requerimientos o requisitos normativos de otro, buscando que se evite debilidades sobre los titulares del derecho en territorios ajenos al nacional. La autoridad competente debe valorar, para otorgar dicha equivalencia, la existencia de un marco legal robusto, mecanismos institucionales de control y recursos efectivos para la defensa de los derechos de los titulares en el país receptor. Este enfoque guarda coherencia con el modelo europeo establecido por el Reglamento General de Protección de Datos (RGPD), el cual también condiciona las transferencias internacionales al reconocimiento de niveles adecuados de protección.

El artículo 45 de la LOPDP establece excepciones, mismas que se aplican cuando sea el caso que el país que va a recibir la información no cumple con las directrices para la protección de datos requerida. En este contexto la transferencia se autorizará siempre y cuando el titular de su consentimiento expreso e informado o por escrito a través de la ejecución de un contrato, mismo que genera una obligación contemplando los intereses. Así la normativa establecida por la legislación ecuatoriana tiene como finalidad mantener la del nivel de protección de datos personales, inclusive fuera del país, garantizando que estos datos fluyan de forma responsable, segura y en el marco del respeto sobre los derechos fundamentales. En otras palabras, la LOPDP aparte de del fortalecimiento sobre la confianza digital y la cooperación internacional, también ubica al Ecuador a un nivel de protección de datos basado en los estándares internacionales de dicha materia.

7.1. Análisis de los capítulos V y IX de la LOPDP

Capítulo V

Dentro de un análisis técnico jurídico, el capítulo V menciona la responsabilidad diferida, esto quiere decir que quien sea responsable sobre la trata de la información será quien

tendrá que garantizar la licitud y transparencia de los procesos, y quien sea el encargado va a obligarse contractualmente sobre la confidencialidad del mismo, también la limitación del propósito y extinción de los datos cuando se concluya el servicio o proceso. Pero, cabe denotar la observancia de vacíos en la regulación los cuales tienen relevancia y pueden afectar la eficiencia normativa.

Esta normativa tiene varios vacíos legales cuando se habla sobre quien es quien, en lo relacionado al manejo de datos, un claro ejemplo de esto vendría siendo la diferencia entre “tercero” y “encargado”, y esto se vuelve un problema cuando hay empresas que subcontratan servicios digitales. Tampoco se sabe bien cuando un acceso a datos cuenta como una trasferencia o no, esto solo empuja a que las empresas actúen en base a su conocimiento general, es decir puede o no estar dentro del marco normativo, también, la ley exige que existan contratos para el tratamiento de datos, pero no menciona como hacerlos, tampoco explica cómo es que la autoridad supervisara estos, de esta manera todo queda a la libre interpretación.

Además, la ley habla de proteger los datos, pero no dice cómo hacerlo en la práctica. No hay reglas claras sobre seguridad digital, cifrado o auditorías, y eso deja mucho espacio para errores o abusos. También hay huecos en el tema del consentimiento en teoría, se pueden usar datos sin pedir permiso en ciertos casos, como emergencias o estudios, pero no se explica bien cómo controlar esos usos ni cómo evitar que se identifique a las personas. En resumen, es una ley que suena bien en el papel, pero en la práctica deja demasiadas dudas y puertas abiertas

Capítulo IX: Transferencia o comunicación internacional de datos personales

Al hablar del capítulo IX de la LOPDP, específicamente del articulo 55 al 61 de esta normativa, hace referencia a la transferencia internacional de datos personales, este tema viene siendo muy importante ya que menciona en sí que se incluye la normativa dentro de un marco global en otras palabras dentro de la globalización digital y por ende en la

economía del dato. La LOPDP se basa en un modelo de adecuación y garantías, el cual tiene parecido al Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Siendo así en el artículo 56, solo se pueden transferir datos a países, organizaciones o entidades que aseguren niveles adecuados de protección, reconocidos mediante resolución motivada de la Autoridad de Protección de Datos Personales.

Los artículos 57 y 58 básicamente dicen que, si un país no tiene buenas leyes para proteger los datos, igual se pueden hacer transferencias siempre y cuando haya reglas o contratos que aseguren que los datos estarán bien cuidados. Es decir, se puede hacer, pero solo si hay garantías parecidas a las nuestras y si las personas todavía tienen forma de reclamar si algo sale mal. Los artículos 59 y 60 hablan de casos más puntuales donde sí se puede compartir información sin tanto requisito, como cuando hay temas de interés público, cooperación entre jueces, cumplimiento de contratos o cosas urgentes que tienen que ver con proteger la vida o la salud de alguien. En resumen, la ley deja unas puertas abiertas, pero con condiciones para que no se abuse de ellas.

Aunque este capítulo parece estar bien desarrollado, en la práctica tiene varios vacios lo cual hace difícil su aplicación. No explica bien cómo se decide si un país tiene un “nivel adecuado de protección” para los datos, dice que eso se verá en el reglamento, pero no da indicios sobre qué criterios o estándares se van a usar. También, habla de cooperación entre autoridades de distintos países, pero no dice cómo se va a hacer, ni cuánto tiempo tienen para actuar así que, si pasa algún problema fuerte con los datos fuera del país, probablemente nadie sepa bien quién debe responder o cómo hacerlo.

También hay problemas con otros temas más técnicos, Las llamadas “normas corporativas vinculantes”, esta no se sabe cómo se aprueban ni qué tanto peso legal tiene si hay un conflicto entre países. Y lo del consentimiento del titular es medio flojo, porque dicen que hay que comunicar los riesgos, pero no aclaran cuáles ni cómo. A eso se le suma, la Autoridad de Protección de Datos tiene que vigilar todo esto, pero la ley no dice si tiene

independencia real ni recursos suficientes, así que viene a ser complicado que pueda controlar todo de forma concreta.

7.2. Reglamento de la LOPDP (2023) y competencias de la Autoridad de Control

El Reglamento General de la Ley de Protección de Datos, aprobado en 2023, es básicamente la guía que explica cómo aplicar en la práctica lo que dice la ley del 2021. Su idea es hacer que los derechos sobre los datos personales realmente se cumplan y que la Autoridad de Protección de Datos pueda hacer su trabajo. Este reglamento pone reglas más claras, define plazos, procedimientos y responsabilidades para las personas o empresas que manejan datos. En pocas palabras, baja a tierra los principios de la ley, como la transparencia, la seguridad y la responsabilidad, para que no se queden solo en teoría, sino que se apliquen de verdad en el día a día.

7.3. Competencias de la Autoridad de Protección de Datos Personales (APDP)

La Autoridad de Protección de Datos Personales (APDP) es como la “policía” de los datos en Ecuador. Se encarga de que se cumpla la ley y de cuidar que nadie use la información personal de forma indebida. Tiene cuatro funciones principales: Supervisar, Regular, Sancionar Y Cooperar. En la parte de supervisión, puede hacer auditorías, pedir información y hasta suspender tratamientos de datos si ve que hay abusos. No solo se trata de no romper la ley, sino de demostrar que se está cumpliendo bien con ella.

La Autoridad de Protección de Datos Personales tiene varias tareas importantes. Primero, se encarga de supervisar y controlar que las personas, empresas o instituciones cumplan con la ley de protección de datos. Para eso puede hacer inspecciones, pedir información, revisar cómo se manejan los datos y, si ve algo raro, ordenar que se corrija o se detenga. También tiene la parte de regular, que significa que puede crear guías y normas más específicas para que todos sepan cómo aplicar correctamente la ley, sobre todo en temas técnicos como la seguridad digital o el uso de datos en el extranjero.

Además, la Autoridad puede sancionar, es decir, poner multas o castigos a quienes no cumplan con las reglas. Sin embargo, todavía hay algunos vacíos sobre cómo se calculan esas sanciones. Por último, también tiene la función de cooperar con otros países y organismos para intercambiar información y trabajar juntos en casos que involucren datos fuera del Ecuador. El problema es que, aunque tiene todas estas funciones, todavía le falta fuerza institucional y recursos para hacerlas efectivas de verdad.

CAPÍTULO II. DERECHO COMPARADO Y ESTÁNDARES INTERNACIONALES EN MATERIA DE TRANSFERENCIA DE DATOS PERSONALES

1. Diferenciación entre transferencia y comunicación internacional de datos.

La correcta diferenciación entre la transferencia internacional de datos personales y la comunicación internacional de datos personales constituye uno de los ejes centrales para garantizar la seguridad jurídica en el tratamiento transfronterizo de información personal. Aunque la Ley Orgánica de Protección de Datos Personales (LOPDP) emplea ambos términos, lo hace de manera ambigua, utilizándolos en ocasiones como sinónimos, lo que genera confusión normativa y dificultades prácticas para los responsables y encargados del tratamiento.

Desde una perspectiva jurídica, ambas figuras implican un flujo internacional de datos; sin embargo, no producen los mismos efectos jurídicos, ni generan iguales niveles de responsabilidad. La distinción resulta fundamental para determinar quién asume el control efectivo sobre los datos, qué obligaciones se activan y qué mecanismos de autorización y garantía deben aplicarse.

La ausencia de una delimitación clara entre estas figuras puede provocar una incorrecta aplicación del régimen de autorización previsto en el Capítulo IX de la LOPDP, así como un debilitamiento de la protección de los derechos del titular, especialmente en contextos de subcontratación internacional, servicios en la nube o cooperación interinstitucional.

1.1. Elementos jurídicos distintivos

Desde el punto de vista jurídico, la transferencia internacional de datos personales se caracteriza por la existencia de un cambio de control y responsabilidad sobre los datos. En este escenario, el responsable del tratamiento en el Ecuador transmite los datos a un destinatario ubicado en el extranjero que pasa a decidir de forma autónoma sobre las finalidades y los medios del tratamiento. En consecuencia, el receptor adquiere la calidad de nuevo responsable del tratamiento, con obligaciones propias frente a los titulares de los datos.

Este cambio de control justifica que la transferencia internacional esté sujeta a requisitos más estrictos, como la exigencia de que el país u organización receptora cuente con un nivel adecuado de protección, o, en su defecto, que se establezcan garantías adicionales aprobadas o supervisadas por la Autoridad de Protección de Datos Personales. La lógica subyacente es evitar que los datos personales queden expuestos a marcos jurídicos más débiles o incompatibles con los estándares ecuatorianos.

Por el contrario, la comunicación internacional de datos personales no implica una cesión de control. En este supuesto, los datos son puestos a disposición de un tercero en el extranjero que actúa por cuenta y bajo las instrucciones del responsable ecuatoriano, sin decidir autónomamente sobre su uso. Jurídicamente, este tercero mantiene la calidad de encargado del tratamiento, y su actuación se encuentra limitada por un contrato u otro instrumento jurídico vinculante.

En la comunicación internacional, el responsable del tratamiento conserva la titularidad del control, así como la responsabilidad principal frente al titular y la Autoridad de Control. El acceso del tercero extranjero a los datos se justifica por razones operativas, técnicas o funcionales, como la prestación de servicios de almacenamiento, soporte tecnológico o procesamiento de información.

La diferencia esencial entre ambas figuras radica, por tanto, en el grado de autonomía decisional del receptor de los datos. Mientras en la transferencia existe independencia y control propio, en la comunicación existe subordinación funcional y ausencia de decisión sobre las finalidades del tratamiento.

1.2. Escenarios prácticos en el sector público y privado

La distinción entre transferencia y comunicación internacional de datos personales se vuelve especialmente relevante al analizar su aplicación en escenarios concretos del sector público y privado, donde el uso de tecnologías digitales y servicios transnacionales es cada vez más frecuente.

En el sector privado, un ejemplo típico de comunicación internacional de datos se presenta cuando una empresa ecuatoriana contrata servicios de computación en la nube con un proveedor extranjero para el almacenamiento o procesamiento de datos de clientes. En este caso, el proveedor actúa como encargado del tratamiento, siguiendo las instrucciones del responsable ecuatoriano y sin utilizar los datos para fines propios. La empresa ecuatoriana mantiene el control sobre la información y debe garantizar contractualmente la confidencialidad, seguridad y limitación del uso de los datos.

En cambio, se configura una transferencia internacional de datos cuando una empresa ecuatoriana remite bases de datos de clientes a una filial o socio comercial en el extranjero que utilizará esa información para sus propias estrategias comerciales, análisis de mercado o prestación directa de servicios. En este supuesto, el destinatario extranjero decide las finalidades y medios del tratamiento, convirtiéndose en responsable autónomo, lo que activa el régimen de autorización y evaluación de nivel adecuado de protección.

En el sector público, la comunicación internacional de datos suele darse en contextos de cooperación administrativa o tecnológica, como el uso de plataformas extranjeras para la gestión de sistemas informáticos estatales o la contratación de servicios de soporte

técnico internacional. Siempre que el proveedor actúe bajo instrucciones precisas y no utilice los datos para fines propios, se mantendrá la figura de comunicación internacional.

Por el contrario, la transferencia internacional se presenta cuando una entidad pública ecuatoriana remite datos personales a organismos internacionales, autoridades extranjeras o entidades supranacionales que los tratarán de manera independiente, por ejemplo, para fines estadísticos, de investigación o de control migratorio. En estos casos, resulta indispensable evaluar el marco normativo del receptor y establecer garantías que aseguren la protección efectiva de los derechos de los titulares.

Estos escenarios evidencian que la falta de una diferenciación clara en la LOPDP genera riesgos de interpretación errónea, ya que operaciones jurídicamente distintas pueden ser tratadas bajo un mismo régimen, debilitando la seguridad jurídica y la tutela de los derechos fundamentales. De ahí la necesidad de una reforma normativa que precise los elementos distintivos y establezca criterios claros para su aplicación práctica.

2. Autorización para la transferencia internacional: requisitos y procedimientos

El avance tecnológico, y el desarrollo comercial en el ámbito digital ha generado un incremento importante en el intercambio de información personal, convirtiéndose en un elemento esencial para la prestación de servicios transnacionales, la cooperación institucional y la gestión empresarial.

2.1. Requisitos para la autorización de la transferencia internacional

La LOPDP exige que toda transferencia internacional de datos personales cumpla con ciertos requisitos que permitan un control adecuado, que evidencie procesos debidamente establecidos, normas claras de protección y garantías que permitan a los titulares acceden de manera precisa a sus derechos, en una síntesis podemos determinar como principales los siguientes:

2.2. Nivel adecuado de protección:

La LOPDP en su artículo 57 detalla que las transferencias internacionales solo pueden realizarse hacia países, organizaciones y personas jurídicas que no:

- Garanticen un nivel de protección adecuado.
- Cumplan debidamente sus obligaciones.
- Se sujeten a la normativa establecida en materia de Protección de Datos Personales y a estándares internacionales de protección.

Es importante que los integrantes del tratamiento de Datos Personales sean conscientes que al país al que requieren transferir datos cuenten con normativa clara que permita a todos un control y correcto tratamiento de los datos personales, esto se fundamenta en que cada integrante debe tener claro sus obligaciones y responsabilidades frente al manejo que deberán tener sobre los datos que deberán ser tratados bajo su responsabilidad sujetándose a principios debidamente establecidos.

2.3. Consentimiento del titular:

Toda transferencia internacional deberá contar con un consentimiento expreso, previo e informado de su titular en el cual se determine con exactitud toda la información para la cual se realizará la transferencia.

2.4. Garantías Contractuales:

Para una correcta transferencia de Datos Personales es importante que dentro de las relaciones contractuales, se generen garantías contractuales de protección que abarquen modelos y procesos establecidos por los integrantes de la protección de datos, en el cual se evidencien de manera clara y precisa las obligaciones, responsabilidades y alcances que deben cumplir para un correcto tratamiento al momento de realizar o recibir la información.

2.5. Autorización por parte de la Autoridad de control:

En los casos donde el país de destino no cuente con normativa que permita garantizar, uno correcto tratamiento y protección dentro de lasa transferencias internacionales de

Datos Personales, quien intervenga será la Autoridad de Protección de Datos Personales con el fin de evaluar y determinar los niveles adecuados de protección, implementando métodos de control, mediante acciones conjuntas con las autoridades de protección de los países destinatarios con la finalidad de proteger, corregir o mitigar un tratamiento indebido o deficiente.

Para este caso la declaración de un nivel adecuado de protección será emitida mediante resolución motivada determinando el proceso adecuado de protección y garantías que correspondan, conforme a lo establecido en la LOPDP:

2.6. Procedimiento para la autorización de la transferencia internacional

Dentro del procedimiento para la autorización es importante determinar dos escenarios frente a la transferencia internacional de Datos Personales, como se ha indicado en el caso de que los países cuenten con un nivel adecuado de protección de Datos Personales y cuenten con normativa legal que fundamente dicha protección, la autorización estará ligada a los procesos internos que los integrantes del tratamiento de Datos Personales establezcan y garanticen para su debido control y este control estará sujeto mediante acuerdos contractuales que delimiten los acuerdos, responsabilidades, obligaciones y alcances que cada integrante asume de acuerdo a su rol dentro del tratamiento, y cada uno se sujete a su legislación en materia de protección de Datos Personales.

De la misma manera tenemos el escenario que el cual el país destinatario no cuente con un nivel adecuado de protección y por ende no genere las garantías debidas para una correcta transferencia, es ahí donde interviene la Autoridad de Control para su debida autorización estableciendo un procedimiento de cumplimiento obligatorio por parte de los integrantes, el cual se define en:

- Un contrato mediante el cual tanto el Responsable como el Encargado se sujeten de manera libre y voluntaria a la normativa ecuatoriana referente a la protección de Datos Personales, aceptando la autoridad y competencia de la Autoridad de Control

de Protección de Datos Personales, y de los tribunales en los casos que aplique.

3. Criterios de “nivel adecuado de protección” en la legislación ecuatoriana

Empecemos definiendo que se entiende por “niveles adecuados de protección”, esto en el contexto de protección de datos personales, quiere decir que cada país debe tener una legislación vigente y reguladora en materia de protección de datos personales, en Ecuador está regulado conforme al Artículo 56 de la LOPDP que expresa sobre la “Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección” y debidamente regulado conforme al Artículo 73 del RGLOPDP que expresa sobre “Criterios de estándares de nivel adecuado de protección”, estos mismo se aplican para la transferencia internacional de datos personales de cada país para definir qué país tiene el nivel adecuado de protección de datos personales, esto en conjunto con lo que establecen la legislación internacional.

¿Entonces se podría decir que Ecuador es considerado como un país a tomar en consideración en temas del nivel adecuado de protección de datos personales? Pues no, ya que a la actualidad no se ha establecido un listado oficial de Países a considerar que cumplen con el nivel adecuado de protección de datos, pero si nos basamos en los lineamientos internacionales y la legislación Ecuatoriana Vigente, Ecuador no podría considerarse como un país calificado para entrar a una lista que cumple con los niveles adecuados de protección de datos personales.

La determinación de “nivel adecuado de protección” de datos personales en sí, es el conjunto de criterios en base a todos los elementos que establece nuestra legislación vigente como: seguridad, confidencialidad y tutela de derechos cuando sean tratado fuera del territorio nacional, en este caso quien determina como autoridad competente quien cumple con estos criterios es la Superintendencia de Protección de Datos Personales, el

nivel adecuado de protección debe en si garantizar el pleno ejercicio de los derechos de los titulares conforme al Artículo 73 del RGLOPDP.

En fin, el nivel adecuado de protección de datos personales no es solo categorizar de manera formal a un país en específico, sino de concretar el cumplimiento de principios constitucionales como lo son de legalidad, finalidad, proporcionalidad, consentimiento, privacidad y la responsabilidad del estado; el cumplimiento de esto da garantía a una confianza digital, sobre todo en temas de transferencias internacional de datos personales.

4. Vacíos y contradicciones detectadas en la LOPDP respecto a la normativa internacional.

La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, marcó un paso decisivo dentro del marco normativo nacional, considerando que su aparición responde a la necesidad urgente de fortalecer la privacidad de los ciudadanos en un contexto actual dentro del cual se ha establecido un uso intensivo de las Tecnologías de la Información y Comunicación, en este sentido, esta Ley vino a superar las limitaciones del antiguo amparo constitucional del habeas data, el mismo que resultaba insuficiente frente a los retos de la nueva era digital.

Al analizar la Ley Orgánica de Protección de Datos Personales se puede observar la influencia del Reglamento General de Protección de Datos de la Unión Europea, ya que, la legislación ecuatoriana adoptó principios y derechos esenciales, incluyendo los de portabilidad y el derecho al olvido, lo cual permitió establecer un marco más alineado con el estándar global de privacidad.

Si bien es cierto se puede decir que, esta inspiración sentó una base robusta en la legislación ecuatoriana, la mera adopción formal del articulado europeo no garantiza su funcionalidad, considerando que el Reglamento General de Protección de Datos de la Unión Europea fue concebido para un modelo económico desarrollado y el tratar de adaptarlo a un contexto legal y socioeconómico en desarrollo como el ecuatoriano, genera

una gran problemática la cual se ve reflejada en desafíos de implementación y vacíos normativos.

El análisis comparativo entre la LOPDP vs. el RGPD y el Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal resulta pertinente, pues estos instrumentos se han consolidado como la normativa general del derecho digital a nivel global

Cabe recordar que el Reglamento General de Protección de Datos de la Unión Europea no se limita a regular la protección dentro de los límites de la Unión Europea, sino que, opera como un instrumento estándar para la adecuación de la normativa internacional debido a su extraterritorialidad y la severidad de su marco sancionatorio.

Por su parte, el Convenio 108 del Consejo de Europa otorga al tratamiento de datos personales la dimensión de derecho humano fundamental, garantizando no solo la protección individual, sino también la libre circulación de la información como elemento esencial en las sociedades modernas.

En este contexto, la efectividad de la LOPDP depende de su capacidad para ofrecer un nivel de protección similar al de los instrumentos internacionales, solo así podrá consolidarse la confianza pública y asegurar la inserción del Ecuador en el flujo económico global de datos.

4.1. Vacíos normativos y contradicciones sustantivas

El estudio de la normativa ecuatoriana permite identificar dos tipos principales de deficiencias:

1. Vacío Normativo. - Hace referencia a la falta de regulación específica sobre una materia que si es cubierta y desarrollada por el derecho internacional.

2. Contradicción Sustantiva. - Esto implica que, las disposiciones normativas del Ecuador establecen un requisito contrario, incongruente o de menor seguridad que el internacional.

4.2. Autonomía de la autoridad de control

La doctrina y la normativa internacional consideran la autonomía institucional de la autoridad de control como un pilar fundamental de la protección de datos.

Artículo 52 RGPD

"1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional."[3]

En este sentido, las autoridades de control deben ser independientes en el ejercicio de sus funciones y competencias, garantizando su capacidad para actuar sin influencia política o económica, lo cual es vital para asegurar la fiscalización objetiva de los responsables del tratamiento de datos.

Por otra parte, la Autoridad Nacional de Protección de Datos Personales en Ecuador ha estado marcada por tensiones respecto a su independencia, ya que inicialmente, esta responsabilidad se encontraba en la Dirección Nacional de Registro de Datos Públicos la cual es parte del Ministerio de Telecomunicaciones y Sociedad de la Información, la cual a su vez es parte del poder ejecutivo.

Actualmente se creó la Superintendencia de Protección de Datos Personales, sin embargo, hay quienes consideran que esta falta de independencia se mantiene debido a la forma de la designación de su máxima autoridad, ya que es elegido de la terna enviada por el ejecutivo al Consejo de Participación Ciudadana y Control Social.

La ausencia de un ente regulador completamente autónomo incrementa el peligro de infracciones a la privacidad, puesto que la fiscalización podría verse comprometida por intereses políticos. En consecuencia, esto mina la confianza de los ciudadanos en la capacidad del Estado para garantizar la protección rigurosa de sus derechos.

[3] Parlamento Europeo y Consejo. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*. *Diario Oficial de la Unión Europea*, L 119/1–88. https://www.boe.es/doue/2016/119/L00001-00088.pdf

4.3. Contradicciones en el Régimen Sancionatorio

El derecho digital internacional, particularmente el RGPD, hace énfasis en la necesidad de que las sanciones impuestas sean efectivas, proporcionadas y, fundamentalmente, disuasorias, para lo cual adopto un criterio de gravedad.

Para las violaciones más graves de los derechos fundamentales y libertades individuales fijó multas máximas que pueden alcanzar el 4% del volumen de negocios global anual del ejercicio financiero anterior o 20 millones de euros, inclinándose por la cantidad mayor, este mecanismo está explícitamente diseñado para ser disuasorio a escala global para las grandes corporaciones multinacionales.

En contraste, el régimen sancionatorio de la Ley Orgánica de Protección de Datos Personales del Ecuador que en su artículo 72 indica:

“Art. 72.- Sanciones por infracciones graves. - La Autoridad de Protección de Datos Personales impondrán las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo:

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

1) Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad

de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad, misma que se establecerá en función a la conducta del infractor; b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales o de ser el caso, de un tercero hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales a un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, se deberá notificar de la resolución con la cual se establezca la infracción cometida la Autoridad de Protección de Datos Personales, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancia las acciones o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.”

Las sanciones graves en el caso de Ecuador se encuentran ligadas al Salario Básico Unificado, lo que fija los topes sancionatorios en valores que no son proporcionales a la capacidad económica del infractor a nivel global.

Mientras que el RGPD utiliza un 4% del volumen de negocios global como base para garantizar la disuasión, la Ley Orgánica de Protección de Datos Personales establece límites fijos, en el caso de servidores públicos con valores que oscilan entre los $ 4700 y

$9400 dólares americanos, incluso para una empresa con un volumen de negocio de 1 millón de dólares, esta limitación se agrava al compararla con la capacidad sancionatoria del marco RGPD, ya que en el Ecuador la sanción sería de entre $ 7000 y $10000 dólares americanos.

La limitación estructural del régimen ecuatoriano provoca un colapso de la disuasión transnacional, ya que, para una empresa multinacional cuya actividad económica se desarrolla principalmente fuera de Ecuador, una multa máxima basada en el SBU o de entre el 0,7% y el 1% del volumen de negocio se concibe como un costo operativo adicional y no como una sanción.

4.4. Transferencia

Los artículos 55 y 56 de la ley Orgánica de Protección de Datos Personales regulan las transferencias internacionales de datos personales, estableciendo la premisa de que los datos solo pueden transferirse a países que ofrezcan un nivel de protección adecuado.

“Art. 55.- Transferencia o comunicación internacional de datos personales. - La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.”

“Art. 56.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección. - Por principio general se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley.”

En principio, esta disposición se alinea con los estándares internacionales, reconociendo la necesidad de asegurar la continuidad del derecho a la privacidad más allá de las fronteras.

Sin embargo, el RGPD introduce mecanismos adicionales de garantía, como las Cláusulas Contractuales Tipo (CCT) y las Normas Corporativas Vinculantes (BCR), cuya aplicación exige un proceso riguroso de evaluación, en este punto, la LOPDP presenta un vacío normativo significativo, pues no incorpora expresamente la obligación de realizar evaluaciones de impacto de la transferencia.

Este requisito cobró relevancia tras la sentencia Schrems II (2020) del Tribunal de Justicia de la Unión Europea, que invalidó el mecanismo de transferencia conocido como Privacy Shield. Dicha decisión impuso la necesidad de verificar si las leyes del país receptor garantizan una protección adecuada frente al acceso gubernamental o la vigilancia masiva.

La ausencia de esta exigencia en la LOPDP genera un problema serio, ya que, las transferencias internacionales podrían basarse únicamente en cláusulas contractuales, sin evaluar si el país de destino ofrece garantías reales frente al uso o acceso indebido de los datos personales, más aún cuando el marco internacional ha dejado claro que las garantías contractuales por sí solas son insuficientes.

4.5. Consideraciones

La promulgación de la Ley Orgánica de Protección de Datos Personales representa, sin duda, un paso decisivo hacia la consolidación de la soberanía digital ecuatoriana, sin embargo; su efectividad depende de la capacidad para armonizar su marco jurídico con los estándares internacionales, particularmente en tres ejes fundamentales:

- Autonomía institucional de la autoridad de control,
- Proporcionalidad y alcance real del régimen sancionatorio, y

- Exigencia de evaluaciones de impacto en transferencias internacionales.

Mientras persistan los vacíos y contradicciones identificados, la LOPDP seguirá ofreciendo una protección incompleta frente a las amenazas del entorno digital contemporáneo, lo cual no solo compromete la seguridad de las personas, sino que también limita la capacidad del Ecuador para integrarse con solidez en el ecosistema global de protección de datos personales.

5. Responsabilidad y sanciones por incumplimiento en la transferencia internacional.

La transferencia internacional de datos personales implica el envío o circulación de información hacia países o entidades fuera del territorio nacional. Este proceso conlleva riesgos muy altos en la garantía de los derechos de los titulares, ya que los datos podrían quedar sujetos a normativas extranjeras con niveles diferentes de protección. La LOPDP establece que las transferencias internacionales solo podrán realizarse hacia países, organismos o entidades que aseguren un nivel adecuado de protección, o bajo mecanismos contractuales que garanticen el cumplimiento de los principios y derechos previstos en la ley.

De acuerdo con el artículo 47 de la LOPDP, el responsable o encargado del tratamiento debe asegurar que el destinatario cumpla con condiciones equivalentes de seguridad y confidencialidad. Asimismo, el artículo 48 exige que toda transferencia se fundamente en garantías adecuadas, tales como cláusulas contractuales tipo o normas corporativas vinculantes. El incumplimiento de estas disposiciones genera responsabilidad para los actores involucrados, que puede ser administrativa, civil o incluso penal, dependiendo de la gravedad del caso y del perjuicio ocasionado.

Según lo dispuesto en el artículo 65 de la LOPDP, la Autoridad de Protección de Datos Personales puede imponer sanciones como: amonestaciones, suspensión de operaciones, eliminación de datos o multas económicas proporcionales a la infracción.

Además, el artículo 66 otorga la facultad a la autoridad a considerar factores como la intencionalidad, la reincidencia y el beneficio económico obtenido para graduar la sanción.

A nivel comparado, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea refuerza esta visión al establecer sanciones que pueden alcanzar hasta el 4 % del volumen global de negocios de la entidad infractora. Este modelo demuestra la relevancia del principio de responsabilidad proactiva, reconocido también en el artículo 26 de la LOPDP, que obliga a los responsables a adoptar medidas técnicas, organizativas y de gobernanza que demuestren el cumplimiento efectivo de la ley.

En este contexto, el régimen ecuatoriano no solo busca sancionar el incumplimiento, sino promover una cultura de cumplimiento y diligencia en el tratamiento de datos personales, especialmente cuando estos se transfieren al extranjero. Como sostiene Daniel J. Solove (2021), la protección de datos debe entenderse como un proceso continuo de gestión de riesgos y rendición de cuentas, más que como un mero cumplimiento formal. Bajo esta perspectiva, la responsabilidad adquiere un carácter preventivo y ético, esencial para garantizar la tutela efectiva del derecho a la protección de datos personales en el entorno digital.

6. EL RGPD: MECANISMOS DE ADECUACIÓN Y EL CONTROL DE LA VIGILANCIA

6.1. La Decisión de Adecuación y las Garantías Apropiadas.

El RGPD establece la transferencia como permitida bajo Decisión de Adecuación (Art. 45) “Transferencias basadas en una decisión de adecuación. - La transferencia de datos personales a un tercer país o a una organización internacional podrá realizarse cuando la Comisión haya determinado que dicho tercer país, territorio o uno o varios sectores específicos dentro de ese tercer país, o la organización internacional en cuestión, garantiza un nivel de protección adecuado. Dicha transferencia no requerirá autorización específica…” o mediante Garantías Apropiadas (Art. 46) “Transferencias sujetas a las debidas garantías.- En ausencia de una decisión de conformidad con el artículo 45 (3), un

responsable o encargado del tratamiento podrá transferir datos personales a un tercer país o a una organización internacional únicamente si ha proporcionado garantías adecuadas y con la condición de que existan derechos exigibles para los interesados y recursos jurídicos efectivos para ellos…".

6.2. El Criterio de la Vigilancia Estatal

La jurisprudencia Schrems II (TJUE) determinó que las garantías contractuales no son suficientes si las leyes de vigilancia extranjera permiten el acceso gubernamental desproporcionado. Esto obliga al exportador a realizar un Transfer Impact Assessment (TIA) para verificar la legislación del país receptor. Este TIA es un requisito de diligencia debida internacional y es el estándar de cumplimiento que debe adoptar la reforma ecuatoriana.

7. EL MARCO DE PRIVACIDAD DE DATOS (DPF) UE–EE. UU.

7.1. El DPF como Estándar de Supervisión y Equivalencia.

El desarrollo del DPF (2023) confirma que la revisión de la vigilancia estatal es el criterio de adecuación más alto. Este acuerdo es la prueba de que el 'Nivel Adecuado de Protección' requiere establecer mecanismos claros y con derecho a recurso para la persona, incluso contra agencias de seguridad nacional.

8. Normativa comparada en América Latina: casos de Colombia, México y Brasil

8.1. MECANISMOS DE DISUASIÓN Y AUTONOMÍA EN AMÉRICA LATINA

Lecciones de Política Regulatoria para Ecuador.

El análisis comparado de la normativa latinoamericana revela dos criterios esenciales de fortalecimiento institucional para Ecuador: i) El modelo sancionatorio de Brasil (multas hasta del 2% del volumen de negocio, superior al 1% ecuatoriano) establece un nivel de disuasión transnacional más efectivo contra grandes corporaciones. ii) La autonomía

funcional de la autoridad de control, ejemplificada por el INAI en México, es clave para la independencia regulatoria.

Tabla de Criterios Comparados La siguiente tabla extrae y contrasta los criterios de los regímenes sancionatorios y la autonomía institucional para definir el estándar que debe alcanzar la LOPDP:

Criterio Clave	Ecuador (LOPDP)	Colombia (Ley 1581)	México (Ley General)	Brasil (LGPD)	Estándar Requerido para Ecuador (Propuesta)
Base de Autorización	Art. 55: Consentimiento, Nivel Adecuado, Cláusulas Contractuales.	Consentimiento, Cláusulas Contractuales, entre otros.	Consentimiento, Cláusulas Contractuales, y otros.	Consentimiento, Cláusulas Contractuales, Entidades Internacionales.	Claridad en la diferencia Transferencia (Responsable) vs. Comunicación (Encargado)
Mecanismo de Verificación (TIA)	No Expreso. (Delegado al Reglamento).	No Expreso.	No Expreso.	No Expreso.	Obligatorio y explícito en la Ley, basado en Schrems II.
Nivel Máximo	1% del volumen de	Multas hasta 2000 SMMLV	Hasta 1,500,000	2% del volumen de	Propuesta de Aumento

de Sanción (Disuasión)	negocio del infractor.	(Mínimo Mensual Legal Vigente).	veces el valor UMA.	negocio del grupo económico.	para disuasión transnacional (ej. 2% o 3% para transferencias ilegales).
Autonomía de la Autoridad	Superintendencia (Reciente, en desarrollo).	Superintendencia de Industria y Comercio (SIC).	INAI (Instituto Nacional de Transparencia ...) - Alto Nivel de Autonomía.	Autoridad Nacional de Protección de Datos (ANPD).	Fortalecer la autonomía funcional y presupuestaria (Modelo INAI).

Es imperativo calificar el resultado de 'Nivel de Disuasión Regional' asignado a Ecuador en esta tabla comparativa, si bien el límite del 1% de la facturación anual es una disuasión Alta para las pequeñas y medianas empresas nacionales; sin embargo, resulta insuficiente para el objetivo de disuasión transnacional que exige el flujo internacional de datos.

El tope del 1% sobre la facturación nacional, a diferencia del 4% sobre el volumen de negocio GLOBAL del RGPD, se concibe como un costo operativo tolerable para las grandes corporaciones, lo cual mina la efectividad del régimen ecuatoriano y justifica la necesidad de aumentar la cuantía sancionatoria para infracciones ligadas a las transferencias internacionales.

8.2. Autoridades de Control y Mecanismos de Supervisión

El éxito y la efectividad de cualquier régimen de protección de datos personales dependen, en gran medida, de la autoridad de control encargada de su aplicación, su capacidad

técnica, la independencia institucional y criterio operativo de estos organismos determinan el nivel real de protección que las leyes pueden ofrecer.

En el contexto latinoamericano, las diferencias en la estructura, autonomía y grado de consolidación de las autoridades de control son notorias, lo que influye directamente en la consistencia y alcance de la fiscalización en cada país.

Estructura y Mandato de las Autoridades

Marco regulatorio y madurez institucional en protección de datos (LATAM)

País	Normativa Principal	Autoridad de Control	Inicio de Vigencia Plena	Grado de Autonomía / Madurez
	LOPDP (2021)	Superintendencia de Protección de Datos Personales	2023 (inicio del régimen sancionatorio)	Baja / En proceso de consolidación
	Ley 1581 (2012)	Superintendencia de Industria y Comercio (SIC)	2012 / 2013	Alta (institución consolidada y activa)
	LFPDPPP (2010) / LGPDPSO (2017)	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)	2010 / 2017	Alta (órgano constitucional autónomo)

	LGPD (2020)	Autoridad Nacional de Protección de Datos (ANPD)	Agosto de 2021	En evolución hacia plena autonomía

En Brasil, la Autoridad Nacional de Protección de Dados ha demostrado un proceso de crecimiento constante hacia la autonomía plena. Su estructura inicial dependía directamente de la Presidencia de la República, pero en los últimos años se han impulsado reformas para dotarla de un estatus de autoridad especial e independiente, con presupuesto y gestión propios. Este avance representa un paso clave hacia la consolidación de un modelo similar al de las autoridades europeas, garantizando imparcialidad y eficacia en la supervisión.

En México, el INAI cuenta con una posición institucional privilegiada, es un órgano autónomo, con competencias consolidadas en transparencia y protección de datos tanto en el ámbito público como privado, lo cual le ha permitido ejercer un control constante y emitir sanciones relevantes, consolidándose como una de las autoridades más activas de la región.

En Colombia, la Superintendencia de Industria y Comercio ha desarrollado una experiencia sólida en la supervisión de datos personales, con amplias facultades de investigación, inspección y sanción. La SIC ha impuesto sanciones ejemplares en casos de incumplimiento, sentando precedentes que fortalecen la cultura de protección de datos y fomentan el cumplimiento preventivo.

Por su parte, Ecuador se encuentra en una etapa de consolidación institucional. La Superintendencia de Protección de Datos Personales, inició sus operaciones en 2023 con la entrada en vigor del régimen sancionatorio. Aunque el marco legal le otorga competencias de regulación, fiscalización, imposición de sanciones, promoción de derechos y emisión de normativa técnica, su capacidad efectiva aún depende del

fortalecimiento de su estructura y la asignación presupuestaria suficiente para su funcionamiento.

El Reto de la Autonomía Institucional

La independencia institucional es un elemento crucial para garantizar que las autoridades de protección de datos puedan ejercer sus funciones sin interferencias políticas o económicas.

Un organismo de control verdaderamente autónomo es capaz de imponer sanciones con objetividad, regular a todos los sectores por igual y promover una cultura de cumplimiento sostenible.

En el caso de Brasil, la ANPD se encuentra en pleno proceso de transición hacia esa independencia plena. Su conversión en una autoridad especial permitirá consolidar un modelo alineado con el europeo, en el cual la separación administrativa y presupuestaria es la clave para el ejercicio eficaz de sus atribuciones. Esta evolución refuerza la legitimidad del sistema y la confianza pública en su capacidad de regulación.

En Ecuador, la situación es más incipiente. Aunque la LOPDP prevé una autoridad de control robusta y técnicamente especializada, su autonomía real aún depende de su desvinculación del poder ejecutivo y de la definición de su estructura administrativa. Actualmente, el procedimiento de designación del Superintendente —propuesto por el Ejecutivo y nombrado por el Consejo de Participación Ciudadana y Control Social— ha sido objeto de debate, pues podría limitar la percepción de independencia del organismo. Pese a ello, se espera que con el tiempo la SPDP logre consolidarse como una entidad técnicamente autónoma y operativamente independiente, capaz de ejercer funciones de supervisión, sanción y orientación con imparcialidad.

La experiencia de países como Colombia y México demuestra que la independencia institucional está directamente vinculada a la efectividad de la fiscalización.

La SIC colombiana, por ejemplo, ha sido capaz de imponer sanciones de alto impacto y dictar directrices interpretativas, lo que ha contribuido a elevar los estándares de cumplimiento empresarial.
Del mismo modo, el INAI mexicano ha mantenido una actividad sancionatoria constante y una fuerte presencia pública, fortaleciendo la confianza de la ciudadanía en su rol.

En este contexto, las empresas multinacionales que operan en Ecuador deben anticipar que, a medida que la Superintendencia alcance su utonoía, el régimen de supervisión y sanción se tornará más riguroso. Las organizaciones deben asumir desde ya una postura de cumplimiento preventivo, documentando sus operaciones, evaluando riesgos y preparando sus procesos internos ante posibles auditorías o investigaciones futuras.

8.3. Régimen Sancionatorio

El grado de efectividad de una ley de protección de datos no depende solo de la solidez de sus principios o del reconocimiento de derechos, sino también de la fuerza disuasoria de su régimen sancionatorio.

En América Latina, las diferencias en la base de cálculo, la proporcionalidad de las multas y la capacidad real de ejecución de las autoridades de control, generan contrastes significativos.

Análisis Comparado del Modelo Sancionatorio

El impacto económico del incumplimiento de las normas de protección de datos varía significativamente de un país a otro, principalmente por el método utilizado para calcular las multas.

Mientras Ecuador y Brasil han adoptado un modelo proporcional al volumen de negocio similar al que aplica el Reglamento General de Protección de Datos, aunque en el caso de Ecuador no tan significativas, México y Colombia continúan aplicando multas con valores fijos.

8.4. Comparación de regímenes sancionatorios:

Cuadro comparativo de sanciones y niveles de disuasión			
País	Base de Cálculo (Sector Privado)	Cuantía Máxima o Porcentaje	Nivel de Disuasión Regional
	Volumen de negocio anual	Hasta el 1% de facturación anual (infracción grave)	Alta (impacto financiero directo)
	Unidades de Valor Tributario (UVT)	Hasta 2.000 Salarios	Alta (sanciones severas)
	Salarios mínimos o pesos mexicanos	Multas hasta MXN 46 millones de pesos	Media – Alta
	Facturación bruta anual	Hasta el 2% hasta $50 millones de reales por infracción	Muy alta (equivalente al RGPD)

Ecuador y Brasil presentan actualmente el mayor potencial de impacto económico para las empresas en caso de infracción a comparación de México y Colombia.

En Ecuador, el régimen sancionatorio de la LOPDP entró plenamente en vigor en mayo de 2023, estableciendo que las infracciones graves pueden acarrear multas de entre el 0,7% y el 1% del volumen de negocios anual, lo que se traduce entre 7000 y 10000 dólares por cada millón de facturación.

Este modelo busca lograr un efecto proporcional al vincular la sanción con la capacidad económica del infractor, además de encontrarse revestida de la facultad de graduar la multa tomando en cuenta la intencionalidad, la reincidencia, el daño ocasionado y el nivel de impacto sobre los derechos de los titulares.

Brasil por otra parte, puede imponer multas de hasta el 2% de la facturación del año anterior, con un límite máximo de 50 millones de reales por infracción, lo cual equivale a un valor aproximado de 9,5 millones de dólares.

En México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha demostrado una supervisión constante y firme. Solo en 2023, las multas impuestas por el INAI superaron los 46 millones de pesos mexicanos (2.5 millones de dólares aproximadamente), lo que refleja un fortalecimiento del régimen y un alto nivel de fiscalización.

En Colombia, la Superintendencia de Industria y Comercio ha mantenido una postura rigurosa, en el caso Worldcoin, mencionado anteriormente, donde se ordenó la clausura definitiva de operaciones por deficiencias graves en la gestión y protección de datos biométricos, se ha convertido en un precedente emblemático para toda la región.

8.5. Transferencias Internacionales de Datos Personales

En un contexto global interconectado, las transferencias internacionales de datos personales se han convertido en uno de los aspectos más complejos de la regulación.

Para las empresas, este proceso constituye un punto crítico, pues implica garantizar que la salida de información del país de origen no reduzca el nivel de protección legal del titular.

En América Latina, aunque los principios fundamentales tienden a ser similares, las herramientas legales y los mecanismos de adecuación difieren entre jurisdicciones, lo que obliga a diseñar estrategias de cumplimiento adaptadas a cada caso.

En Ecuador, las transferencias internacionales de datos personales están condicionadas al cumplimiento de estándares internacionales, así como a los principios rectores establecidos en la Ley Orgánica de Protección de Datos Personales.

En todos los casos, el responsable del tratamiento debe garantizar que el nivel de protección se mantenga equivalente al del país de origen, evitando que los datos queden expuestos a legislaciones menos estrictas.

Mecanismos de Adecuación Comparados

Las jurisdicciones analizadas difieren sustancialmente en la forma en que evalúan la adecuación del país receptor y en los mecanismos utilizados para legitimar las transferencias.

- Colombia: Su Ley 1581 de 2012 establece que la transferencia solo puede realizarse hacia países que cuenten con un “nivel adecuado de protección”, de acuerdo con una lista definida por la autoridad competente, la Superintendencia de Industria y Comercio (SIC). Además, incluso cuando el país receptor sea considerado adecuado, la transferencia debe ir acompañada del consentimiento del titular, salvo excepciones específicas previstas en la ley.
- Brasil y Ecuador: Ambos países siguen un enfoque contractual inspirado en el RGDP. En Brasil, la Lei Geral de Proteção de Dados (LGPD) permite el uso de Cláusulas Contractuales Tipo (CCT) o Normas Corporativas Vinculantes (BCR), mediante las cuales las partes se comprometen a mantener estándares de seguridad y confidencialidad equivalentes a los de la ley brasileña.

  En Ecuador, aunque la LOPDP no establece formalmente una lista de países con nivel adecuado de protección, sí exige que toda transferencia internacional cumpla con los principios del marco nacional y con los estándares internacionales

reconocidos, lo que en la práctica obliga a recurrir a instrumentos contractuales o mecanismos de certificación para sustentar la legalidad del proceso.

En ambos sistemas, el cumplimiento no se limita a la existencia de una cláusula contractual, sino que requiere la verificación documentada de las condiciones reales del tratamiento en el país receptor, incluyendo aspectos de ciberseguridad, confidencialidad y supervisión.

Las diferencias entre el enfoque legal generan grandes desafíos para las empresas, ya que, al gestionar flujos de datos transfronterizos dentro de la región, implica que deben adoptar medidas diferentes desde el país de origen hacia el país receptor, por ejemplo, si se transfieren datos desde Ecuador hacia Colombia se deben cumplir los principios establecidos en ambos territorios ya que difieren sobre su tratamiento basado en garantías contractuales el primero y en el consentimiento expreso en el segundo, lo cual obliga a la empresa a implementar una doble validación legal para asegurar que la transferencia sea válida tanto en el país de origen como en el de destino.

De lo expuesto se colige que, aunque los países latinoamericanos comparten una visión común en torno a la protección de datos, no cuentan con una normativa armonizada que permita un mejor flujo de datos, lo cual genera costos adicionales para su cumplimiento.

9. Directrices internacionales relevantes

Las Directrices de la OCDE de 1980 fueron uno de los primeros intentos internacionales por poner reglas sobre cómo manejar los datos personales. En ese tiempo, la tecnología empezaba a crecer rápido y la información ya no se quedaba en un solo país, lo que hacía que cada Estado tuviera sus propias normas y todo fuera un desorden. Por esta razón, la OCDE quiso encontrar un punto medio entre permitir que la información circule libremente y proteger la privacidad de las personas, buscando que los países tuvieran criterios parecidos y no se complicaran entre sí.

Estas directrices no eran leyes obligatorias, sino una especie de guía con principios para que cada país los adaptara según su realidad. Eso ayudó a que muchos las aceptaran rápido, porque no imponían reglas estrictas, sino recomendaciones para trabajar en conjunto y generar confianza. De cierta forma, la OCDE se adelantó al problema actual de cómo manejar el flujo de datos entre países sin poner trabas al comercio ni poner en riesgo la privacidad.

En otras palabras, las Directrices de 1980 buscaron mantener un equilibrio para proteger la información personal como un derecho de cada individuo, pero sin frenar el intercambio internacional de datos. Centrándose en los datos que se procesan de forma automática y aplicaron tanto para instituciones públicas como privadas. La idea principal era simple pero poderosa ya que los datos personales le pertenecen a la persona, y su manejo debe hacerse con respeto y responsabilidad, sin impedir el desarrollo tecnológico ni económico.

9.1. Principios fundamentales

Las Directrices de la OCDE se basan en ocho principios que marcaron la base de casi todas las leyes modernas sobre protección de datos. En resumen, dicen que los datos personales deben obtenerse de forma legal y con permiso, usarse solo para lo que se dijo desde el inicio y mantenerse correctos, actualizados y seguros. También, las personas tienen derecho a saber qué información se guarda sobre ellas, a corregirla o eliminarla si está mal, y las empresas o instituciones deben hacerse responsables de cumplir con todo eso. Estos principios buscan que la privacidad no sea solo que nadie se meta en tu vida, sino también que existan reglas claras y acciones concretas para protegerla.

9.2. Convención 108+ del Consejo de Europa

La Convención 108+ es una versión actualizada del primer tratado internacional sobre protección de datos, creado en 1981. Fue modernizada en 2018 porque la tecnología ha cambiado muchísimo y ahora los datos personales circulan por todo el mundo en entornos digitales. Esta nueva versión busca asegurar que los derechos de las personas sigan

protegidos frente al uso masivo de información, manteniendo su carácter obligatorio para los países que la adopten. Así, se convierte en una referencia mundial que busca un mismo nivel de protección sin importar el país.

La Convención incluye principios más modernos, como la transparencia, la responsabilidad y la protección de los datos desde el diseño. También reconoce derechos nuevos, como el de no ser juzgado solo por decisiones automáticas sin participación humana y el derecho a mover tus datos de un servicio a otro. Esta exige que las autoridades de control sean más fuertes y puedan cooperar entre países, ya que los datos hoy cruzan fronteras fácilmente y se necesita coordinación para protegerlos bien.

Más allá de lo técnico, esta Convención tiene un enfoque ético y humano. Su mensaje es claro que la tecnología debe servir a las personas y no al revés. Busca que los avances digitales respeten la dignidad y los derechos de cada individuo. Aunque depende de la voluntad de los países para aplicarla bien, la Convención 108+ se considera un modelo global para garantizar la privacidad, la confianza y la justicia en la era digital.

9.3. Estándares de la OEA sobre privacidad y protección de datos

Los Estándares de la OEA sobre privacidad y protección de datos, creados en 2021, buscan que los países de América Latina y el Caribe tengan reglas parecidas para cuidar la información personal. La idea es que todos protejan la dignidad y los derechos de las personas, pero sin frenar el avance tecnológico. Estos lineamientos se enfocan en que los datos se usen solo con fines claros y legales, que sean correctos, seguros y que las personas puedan saber quién los tiene y para qué. También resaltan la importancia de tener autoridades independientes que vigilen y hagan cumplir las normas.

Estos estándares tratan de conectar las políticas europeas con la realidad latinoamericana, buscando un punto medio entre proteger los derechos humanos y permitir la innovación digital. Más que poner límites, promueven una cultura de confianza y responsabilidad en el manejo de la información. En el fondo, lo que plantean es que la

privacidad no solo sirve para evitar abusos, sino que también es una base importante para mantener una democracia sana en esta nueva era digital.

10. Análisis comparativo entre la LOPDP, el RGPD y el DPF

10.1. Cuadro comparativo de principios, procedimientos y sanciones

	LOPDP (Ecuador)	RGPD (Unión Europea)	DPF (Data Privacy Framework – EE. UU.)
Principios rectores	Legalidad, lealtad, transparencia, finalidad, proporcionalidad, minimización de datos, exactitud, confidencialidad y responsabilidad proactiva (art. 7).	Licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; responsabilidad proactiva (art. 5).	Aviso, elección, responsabilidad por transferencias posteriores, seguridad, integridad de los datos, acceso y recurso independiente.
Base legal para el tratamiento y la transferencia internacional	Consentimiento expreso o existencia de garantías adecuadas en el	Transferencias permitidas solo a países con nivel adecuado de protección o	Basado en la adhesión voluntaria de las empresas estadounidenses

	país receptor (arts. 47–48).	mediante cláusulas contractuales tipo, normas corporativas vinculantes o consentimiento (arts. 44–50).	a los Principios del DPF y supervisión por el Departamento de Comercio de EE. UU.
Derechos del titular o interesado	Acceso, rectificación, eliminación, oposición, portabilidad y limitación del tratamiento (arts. 20–26).	Idénticos derechos (denominados "derechos ARCO+"); incluye derecho a la portabilidad y a no ser objeto de decisiones automatizadas.	Derechos de acceso, corrección y eliminación frente a entidades certificadas; canal de reclamación ante organismos independientes o la FTC.
Autoridad de control	Autoridad de Protección de Datos Personales (ente adscrito a la Función Ejecutiva).	Autoridades nacionales de protección de datos (supervisores independientes) y el Comité Europeo de	Departamento de Comercio de EE. UU. y la Comisión Federal de Comercio (FTC), con mecanismos de revisión por el

		Protección de Datos.	panel arbitral del DPF.
Procedimientos de reclamo y control	Reclamo ante la Autoridad; posibilidad de medidas correctivas y sancionatorias.	Sistema jerarquizado: reclamo ante el responsable, luego ante autoridad nacional y, finalmente, vía judicial.	Sistema escalonado: reclamo ante la empresa, luego ante organismos independientes y finalmente ante la FTC o panel arbitral.
Sanciones por incumplimiento	Amonestaciones, suspensión o eliminación de datos, multas administrativas proporcionales (hasta 1% de ingresos anuales o 0,7 millones USD aprox.).	Multas de hasta 20 millones de euros o el 4% del volumen global de negocios; medidas correctivas y prohibición de tratamiento.	Pérdida de certificación, sanciones administrativas de la FTC y prohibición de transferencias desde la UE.
Enfoque general	En fase de implementación y consolidación institucional; busca armonizarse con	Marco consolidado, con fuerte orientación a la protección integral del individuo.	Mecanismo de autorregulación supervisada, orientado a garantizar flujos

	estándares internacionales.		transatlánticos seguros de datos.

CAPÍTULO III. PROPUESTA DE REFORMA A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

1. FUNDAMENTACIÓN DE LA PROPUESTA Y CRITERIOS OBLIGATORIOS

1.1 Fundamento Jurídico: El Principio Pro Homine y Schrems II

La propuesta de reforma se fundamenta en el Principio Pro Homine (Art. 417 de la Constitución) y en la obligación de armonizar el derecho nacional con los más altos estándares internacionales, como el RGPD. La jurisprudencia Schrems II del Tribunal de Justicia de la Unión Europea demostró que la protección contractual es inútil si la ley del país receptor permite la vigilancia masiva. Por lo tanto, la LOPDP debe ser reformada para incorporar este requisito de control. 1.2. Inclusión del Transfer Impact Assessment (TIA) Para subsanar el vacío identificado en la Ley, se exige legalmente la incorporación de la Evaluación de Impacto de Transferencia (TIA). Este instrumento es indispensable para que el responsable demuestre que las cláusulas contractuales son efectivas frente a la legislación de vigilancia del país receptor, cumpliendo con la debida diligencia exigida por los estándares globales. 1.3. Criterios de Rechazo por Ley y Distinción Conceptual Se incorpora un mandato legal expreso para la Superintendencia de Protección de Datos Personales, obligándola a rechazar la adecuación si la legislación extranjera es desproporcionada. Asimismo, la propuesta legal clarifica la distinción conceptual entre Transferencia (cambio de responsable) y Comunicación (acceso por un encargado).

1.2. Criterios jurídicos esenciales

Con base en el modelo europeo y en las directrices OCDE (1980), se propone que la Autoridad ecuatoriana adopte los siguientes criterios mínimos:

1.2.1. Existencia de un marco normativo integral

El país receptor debe contar con una legislación que regule el tratamiento de datos personales, establezca principios rectores como licitud, transparencia, proporcionalidad y minimización, y otorgue derechos exigibles a los titulares (Garrido, 2020).

1.2.2. Garantía efectiva de derechos

Los derechos de acceso, rectificación, supresión, oposición y portabilidad deben ser materialmente ejercitables mediante mecanismos administrativos o judiciales (Bertoni, 2018).

1.2.3. Autoridad de control independiente

El RGPD exige que la autoridad nacional cuente con autonomía, recursos propios y facultades sancionadoras (art. 52 RGPD). Sin esta garantía institucional, el nivel adecuado no puede ser reconocido.

1.2.4. Régimen sancionatorio proporcional y disuasorio

Las sanciones deben tener la capacidad real de prevenir infracciones, lo cual implica multas proporcionales al impacto del tratamiento y a la capacidad económica del infractor (Kuner, 2020).

1.3. Criterios técnicos mínimos

Además de los aspectos jurídicos, el nivel adecuado de protección requiere demostrar que el país o entidad receptora dispone de medidas tecnológicas que garanticen la integridad y seguridad de los datos:

1.3.1. Medidas de seguridad equivalentes a estándares internacionales

Debe verificarse la existencia de políticas basadas en ISO/IEC 27001, NIST o marcos similares, que establezcan controles de seguridad, gestión de incidentes y auditorías periódicas (Villarreal, 2022).

1.3.2. Evaluaciones de impacto y gestión de riesgos

La realización de evaluaciones de impacto (DPIA) constituye un estándar exigido por el RGPD y considerado indispensable para identificar riesgos en transferencias internacionales (CEPD, 2021).

1.3.3. Registro y trazabilidad

El país receptor debe contar con sistemas para registrar accesos, detectar violaciones y notificar brechas a autoridades y titulares, conforme a buenas prácticas internacionales (Garrido, 2020).

1.4. Relevancia para la reforma legislativa

La incorporación explícita de estos criterios en la LOPDP es fundamental para alinear la normativa ecuatoriana con los estándares globales de protección de datos. Asimismo, fortalece la confianza digital, mejora la interoperabilidad con países que ya aplican modelos maduros y asegura la protección efectiva de los derechos de los titulares más allá de las fronteras nacionales.

La reforma no solo clarificaría la interpretación de los artículos 56–61 de la LOPDP, sino que además dotaría a la Autoridad de Control de herramientas objetivas para tomar decisiones técnicas, jurídicas y verificables. Con ello, Ecuador avanzaría hacia un sistema coherente y alineado con el paradigma internacional de protección de datos personales.

2. Propuesta articulada de modificación a los Capítulos V y IX de la LOPDP

CAPITULO V

Artículo 33. – Definiciones. -

a) Comunicación de datos personales. - Para efectos de la LOPDP, se entenderá por comunicación de datos personales toda entrega, revelación y/o puesta a disposición de datos personales a un tercero por parte del responsable del tratamiento, sin que ello signifique la facultad de realizar el tratamiento por parte del

tercero, estos datos serán exclusivamente utilizados de manera informativa de acuerdo con la finalidad previamente determinada entre el responsable y el tercero. No constituirá comunicación de datos personales, la entrega de datos al Encargado del tratamiento cuando este actúe de acuerdo a lo determinado por el Responsable por intermedio de un contrato de encargo.

b) Transferencia de datos personales. - Para efectos de la LOPDP, se entenderá por transferencia de datos personales toda cesión, transferencia y/o entrega de datos personales, realizada por el Responsable del tratamiento a un tercero, permitiendo al tercero la facultad de realizar para las finalidades determinadas contractualmente, las que no dependen exclusivamente del responsable y/o para fines propios el tratamiento a los datos personales por su propia cuenta.
Toda comunicación y transferencia de datos personales requerirán de consentimiento informado del titular, salvo las excepciones previstas en la LOPDP.

Artículo innumerado. - Aspectos que distinguen la comunicación con la transferencia de datos personales.

La Autoridad de Control y los Responsables del tratamiento deberán considerar los siguientes aspectos para determinar cuándo constituye comunicación o transferencia de datos personales:

1. Finalidad:
    - Se entenderá por comunicación de datos personales cuando la finalidad por la cual se entregó la información al tercero está vinculada al cumplimiento de una actividad puramente informativa establecida por el Responsable.
    - Se entenderá transferencia de datos personales cuando la finalidad por la cual se transmitió la información al tercero está determinada

contractualmente, no dependen del Responsable y podrá ser utilizada para fines propios del tercero, transfiriendo la responsabilidad de protección.

2. Nivel de control:
    - En los casos que correspondan por comunicación de datos personales el Responsable determinará sus finalidades únicamente con carácter informativo sin establecer medios ni finalidades para el tratamiento de datos personales.
    - En los casaos que correspondan por transferencia de datos personales el Responsable determinará las finalidades con el objetivo de cumplir obligaciones contractuales, así mismo cuando el tercero adquiera control sobre las finalidades a desarrollar y los medios que utilizará para el tratamiento de los datos personales
3. Autonomía del tercero:
    - Se considera Comunicación de datos personales cuando la actuación del tercero sea de manera subordinada a lo establecido por el Responsable.
    - Se considera Transferencia de datos personales cuando la actuación del tercero se derive a autónoma ya que podrá integrar los datos transmitidos en sus propias bases, sistemas o procesos para realizar un tratamiento independiente.
4. Naturaleza de la relación jurídica:
    - Habrá comunicación cuando el tercero no adquiera nuevas facultades de uso de los datos.
    - Habrá transferencia cuando el tercero reciba facultades de tratamiento ampliadas respecto del responsable.

Art. 34.- Transferencia o comunicación de datos personales. -

Los datos personales se podrán comunicar o transferir en los siguientes casos:

a) Cuando el Responsable del tratamiento cuente con el consentimiento de su titular, debidamente informado, en el que se deberá especificar si se trata de comunicación o de transferencia, salvo las excepciones previstas en la presente Ley.
b) Cuando exista un interés legitimo para que se produzca la comunicación o la transferencia de datos personales.
c) Cuando exista una finalidad especifica relacionada con el Responsable y el tercero (destinatario).
d) Cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley

Art. 35.- Acceso a datos personales por parte del encargado.- Se considerará exclusivamente acceso a datos personales por parte del encargado cuando este acceda a datos personales para el cumplimiento de la prestación de un servicio directamente hacia el responsable del tratamiento de datos, por tanto el tercero que ha accedido legítimamente a datos personales bajo estas circunstancias será considerado encargado del tratamiento y no se podrá considerar comunicación ni transferencia de datos personales.

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara, precisa y delimitada que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.

El encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales. -

No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:

1) Cuando los datos han sido recogidos de fuentes accesibles al público;

2) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;

3) Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;

4) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y,

5) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.

6) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado, una vez pasada la urgencia de interés público.

Cuando sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, este puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna.

La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de (sic)

Art (innumerado). – Lineamientos técnicos sobre comunicación y transferencia.

Para que exista una correcta diferenciación y aplicación entre comunicación y transferencia de datos personales, la Autoridad de Protección de Datos Personales será quien elabore una guía técnica en la que consten procesos prácticos y metodologías de evaluación de riesgos.

Art. (innumerado). - Del Registro obligatorio

El responsable del tratamiento de Datos personales deberá registrar en debida forma el tipo de operación que va a realizar, de acuerdo a los parámetros establecidos por la Autoridad de Control entre:

- Comunicación de Datos Personales
- Transferencias de Datos Personales nacionales,
- Transferencias de Datos Personales internacionales;

- Acceso a Datos Personales por encargo.

Art 37.- Sanciones por incumplimiento. -

El registro incorrecto por parte del Responsable del Tratamiento de Datos personales en clasificar correctamente una comunicación o transferencia de datos personales sea esta nacional o internacional, se considerará una infracción grave y dará lugar a sanciones administrativas que correspondan.

CAPITULO IX

Artículo 55.- Consideraciones generales. -

La comunicación o la transferencia internacional de datos personales se sujetarán a lo previsto en el presente capítulo, esta Ley y a la normativa especializada en la materia, garantizando siempre el efectivo derecho a la protección de datos personales.

Art. 56.- Transferencia internacional de datos personales a países con nivel adecuado de protección. -

Por principio general se podrán transferir datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley.

Cuando resulte necesario por la naturaleza de la transferencia, la Autoridad de Protección de Datos Personales podrá implementar métodos de control ex post que serán definidos en el Reglamento a la Ley. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países.

Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la que se establezca que

la transferencia o comunicación internacional de datos personales cumple niveles adecuados de protección o de garantías adecuadas de protección, conforme a lo establecido en esta ley y su reglamento.

Art. 57.- Transferencia internacional de datos personales mediante garantías adecuadas. –

En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no cuente con un nivel adecuado de protección, se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente:

a. Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente.

b. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,

c. El derecho a solicitar la reparación integral, de ser el caso.

Para que ello ocurra, la transferencia internacional de datos personales se sustentará en un instrumento jurídico que contemple los estándares antes determinados, así como aquellos que establezca la Autoridad de Protección de Datos Personales, el mismo que deberá ser vinculante.

Art. 58.- Normas corporativas vinculantes. -

Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales, normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, las cuales deberán cumplir las siguientes condiciones:

1. Será de obligatorio cumplimiento para el responsable del tratamiento y para la empresa a la que eventualmente transfieran datos personales.

2. Brindar a los titulares los mecanismos adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales observando las disposiciones de la presente ley;

3. Incluir una enunciación detallada de las empresas filiales que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además, se incluirá la estructura y los datos del contacto del grupo empresarial o joint venture, dedicadas a una actividad económica conjunta y de cada uno de sus miembros.

4. Incluir el detalle de las empresas encargadas del tratamiento de datos personales, las categorías de datos personales a ser utilizados, así como el tipo de tratamiento a realizarse y su finalidad;

5. Observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes;

6. Contener la aceptación por parte del responsable o del encargado del tratamiento de los datos personales, o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si demuestra que el acto que originó la violación no le es imputable;

7. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes;

8. Incluir las funciones de todo delegado de protección de datos designado de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas

corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control así como los mecanismos y procesos de supervisión y tramitación de reclamaciones;

9. Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirán auditorías de protección de datos, y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán comunicados al delegado de protección de datos designado de conformidad con la presente ley, o cualquier otra entidad o persona encargada del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o empresas afiliadas dedicadas a una actividad económica conjunta y al Directorio de la empresa que controla un grupo empresarial, y a disposición de la Autoridad de protección de datos personales:

10. Incluir los mecanismos para cooperar de forma coordinada con la autoridad de protección de datos personales y el responsable del tratamiento de los datos personales; y,

11. Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.

Cualquier cambio a ser realizado a estas normas deberá ser notificado a la autoridad de protección de datos personales y al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud.

Art. 59.- Autorización para transferencia internacional. -

Para todos aquellos casos no contemplados en los artículos precedentes, en los que se pretenda realizar una transferencia internacional de datos personales, se requerirá la autorización de la Autoridad de Protección de Datos, para lo cual, se deberá garantizar documentadamente el cumplimiento de la normativa vigente sobre protección de datos de carácter personal, según lo determinado en el Reglamento de aplicación a la presente Ley.

Sin perjuicio de lo anterior la información sobre transferencias internacionales de datos personales deberá ser registradas previamente en el Registro Nacional de Protección de Datos Personales por parte del responsable del tratamiento o, en su caso, del encargado, según el procedimiento establecido en el Reglamento de aplicación a la presente Ley.

Art. 60.- Casos excepcionales de transferencias internacionales. -

Sin perjuicio de lo establecido en los artículos precedentes se podrá realizar transferencias internacionales de datos personales, en los siguientes casos:

1. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable;

2. Cuando el titular haya otorgado su consentimiento explícito a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas.

3. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;

4. Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;

5. Cuando la transferencia sea necesaria por razones de interés público.

6. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional.

7. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones

8. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;

9. Cuando se realicen transferencias de datos en operaciones bancarias y bursátiles.

10. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos; y,

11. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

Art. 61.- Control continuo. -

La Autoridad de Protección de Datos Personales realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.

En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente Ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán

transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

5. Impacto jurídico y social de la reforma propuesta.

El impacto jurídico que presenta la propuesta de reforma a los capítulos V y IX de la Ley Orgánica de Protección de Datos Personales es significativo, ya que busca corregir vacíos y contradicciones legales existentes. Además, reconoce que el intercambio de información es una parte primordial de la economía digital y, por ello, propone establecer normas claras entre el Estado, las organizaciones y los titulares de los datos personales. Todo ello resulta coherente con los estándares internacionales aplicables a la transferencia o comunicación internacional de datos personales, fortaleciendo la seguridad jurídica y generando un entorno atractivo para la inversión (Kuner, 2020; Bertoni, 2018).

La propuesta de reforma dotará de mayor seguridad jurídica al responsable y al encargado del tratamiento de datos personales, ya que delimita los conceptos de cuándo se considera transferencia internacional y cuándo se considera comunicación internacional de datos personales. Esta claridad al definir ambas figuras evitará las “zonas grises” que pueden comprometer la seguridad jurídica y la tutela efectiva del derecho a la protección de datos personales, tal como advierte Piñar Mañas (2018).

Asimismo, al establecer esta propuesta de reforma se busca una armonización con los estándares internacionales, conforme a las normativas analizadas durante el proyecto, como el Reglamento General de Protección de Datos (RGPD), el Data Privacy Framework y el Convenio 108+. Esta armonización permite avanzar hacia la llamada “interoperabilidad normativa”, evitando que existan debilidades en la protección de datos personales cuando la información cruce fronteras (Bertoni, 2018; Bygrave, 2021).

Finalmente, la reforma otorgará mayor eficiencia y eficacia a la Autoridad de Protección de Datos Personales al definir procesos más claros para la evaluación y resolución de autorizaciones de transferencia internacional. Esto se alinea con lo previsto en los

estándares globales sobre el rol técnico y autónomo de las autoridades de control (Bygrave, 2021).

En cuanto al impacto social, la reforma generará un mayor empoderamiento para el titular de los datos personales, ya que le permitirá conocer dónde se encuentran sus datos, quién los controla y qué tipo de protección reciben tanto dentro como fuera del país. Este incremento en la transparencia fortalecerá la confianza digital, necesaria para el uso de servicios electrónicos y la participación en plataformas internacionales. A su vez, esta confianza promueve la competitividad del país en el mercado digital y genera mayor seguridad para los inversionistas (Solove, 2021; OCDE, 2022).

6. Viabilidad y beneficios esperados

La propuesta de reforma demuestra ser viable en los planos jurídico, institucional, técnico y económico. Desde la perspectiva jurídica que es el eje central del presente proyecto su validez se fundamenta en los principios constitucionales que reconocen el derecho a la autodeterminación informativa, previstos en el artículo 66, numeral 19, así como en los principios de privacidad y seguridad jurídica establecidos en los artículos 18 y 76 de la Constitución de la República del Ecuador.

Al mismo tiempo, la propuesta se articula con estándares internacionales que ya sirven como referencia para el legislador ecuatoriano, especialmente el Reglamento General de Protección de Datos de la Unión Europea y el Data Privacy Framework entre la UE y los Estados Unidos. Esta alineación permite reducir incertidumbres normativas y facilita la solución de posibles controversias relacionadas con el envío y tratamiento de datos personales fuera del país.

Otro elemento que reafirma su viabilidad es que no contradice tratados internacionales ni implica la modificación integral de la normativa vigente. Se trata de una reforma puntual a los artículos correspondientes a los Capítulos V y IX de la Ley Orgánica de Protección de

Datos Personales, por lo que no requiere un proceso legislativo complejo ni una derogación total de la ley. Esto favorece una aprobación más ágil y disminuye la carga de ajustes institucionales.

En términos prácticos, la reforma aportará mayor seguridad jurídica y fortalecerá la confianza en el entorno digital ecuatoriano. Un marco normativo más claro y alineado con estándares globales permitirá que Ecuador sea visto como un país con condiciones adecuadas para la transferencia internacional de datos, lo que puede traducirse en un mejor flujo de información, crecimiento del comercio electrónico y mayor inversión en infraestructura tecnológica.

Entre los principales beneficios se destacan:

- la reducción de riesgos derivados de vacíos o contradicciones normativas;
- una delimitación más clara entre transferencia y comunicación internacional de datos personales;
- mecanismos mejor definidos para evaluar la seguridad del tratamiento en el extranjero; y
- un entorno más confiable para empresas tecnológicas y para actividades digitales que dependen del manejo de datos.

Todo ello contribuye a un ecosistema digital más seguro y competitivo, en un contexto donde el comercio electrónico y los servicios en línea continúan expandiéndose de manera acelerada.

CAPÍTULO IV. CONCLUSIONES, RECOMENDACIONES Y CONTRIBUCION DE LA INVESTIGACION

1. Conclusiones generales de la investigación

En conclusión, la Constitución de la República del Ecuador nos dio los elementos necesarios y suficientes para establecer lineamientos normativos para el tema de protección de datos personales, tal es así que implemento en el año 2021, la Ley Orgánica de Protección de dato personales y a su vez su reglamento, lo cual visibiliza su intención de alinearse a una protección que se sujeta a estándares internacionales, en donde se garantizan derechos y libertades fundamentales de las personales naturales como titulares de su información, pero aun así existen vacíos jurídicos y ambigüedades en especial a lo referente el tema de transferencia o comunicación internacional de datos personales; lo cual no permite una correcta aplicación de la normativa existe.

El análisis comparado con diferentes legislaciones vigentes en cada país y en especial a las legislaciones más avanzadas en el tema de protección de datos como son el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y el Marco de Privacidad de Datos UE–EE. UU. (Data Privacy Framework), dan a entender que Ecuador siguió parte de estos lineamientos normativos.

Por último, el planteamiento del presente trabajo de investigación va encaminado en reformar capítulos de la Ley Orgánica de protección de datos personales y orientar de forma correcta la aplicación de transferencia internacional de datos personales y la comunicación internacional de datos personales.

La Ley Orgánica de Protección de Datos Personales de Ecuador, a pesar de su alineación con el modelo europeo, presenta vacíos técnicos y contradicciones estructurales que no son simples reflejos de un sistema en crecimiento, sino una vulnerabilidad jurídica que compromete la continuidad de la protección de los derechos fundamentales de los ciudadanos ante el flujo internacional de datos.

Conclusión General 1

La Ley Orgánica de Protección de Datos Personales presenta un vacío de seguridad jurídica sustancial al no diferenciar, definir ni regular de forma clara e independiente los

conceptos de "comunicación internacional de datos personales" y "transferencia internacional de datos personales". Este uso indistinto en el articulado compromete la eficacia de la norma, dificulta la correcta aplicación de los regímenes de autorización y sanción, y genera incertidumbre en las obligaciones de cumplimiento para los responsables y encargados del tratamiento de datos, debilitando la capacidad de la Autoridad de Control para ejercer una fiscalización objetiva y precisa sobre los flujos transfronterizos.

Conclusión General 2

El análisis comparado con marcos normativos internacionales, especialmente el RGPD, demuestra que el marco legal ecuatoriano es insuficiente al delegar a un reglamento posterior la determinación de los criterios para declarar un nivel adecuado de protección.

Esta insuficiencia radica en la falta de un mandato legal expreso que obligue a la autoridad de control a evaluar rigurosamente el estado de derecho y las leyes de vigilancia masiva o desproporcionada en el país receptor, tal como exige la jurisprudencia Schrems II.

En consecuencia, la actual configuración del procedimiento no garantiza que el nivel de protección de los derechos de los titulares sea equivalente al ecuatoriano una vez que los datos abandonan el territorio nacional, lo cual es contrario al principio de continuidad de la protección.

Conclusión General 3

La propuesta de reforma, sustentada en el derecho comparado y centrada en la redefinición conceptual de la comunicación y transferencia, y en la obligatoriedad de un mecanismo de evaluación de impacto que al menos sea similar al Transfer Impact Assessment, se establece como una solución necesaria y viable. Esta implementación dotaría al Superintendente de Protección de Datos de las herramientas técnicas y jurídicas indispensables para evaluar los riesgos de injerencia en los derechos de los titulares.

De esta manera, el Ecuador avanzaría hacia la armonización con los estándares internacionales, asegurando que los flujos transfronterizos de datos se realicen bajo un esquema de máxima garantía de los derechos fundamentales de los ciudadanos.

2. Conclusiones específicas por capítulo

2.1. Conclusión del Capítulo I

a) El estudio concluye que el derecho a la protección de datos personales se encuentra firmemente establecido como un derecho fundamental, tanto a nivel constitucional en el Ecuador como en el marco normativo internacional. La Ley Orgánica de Protección de Datos Personales actúa como el instrumento principal de tutela, elevando la materia al rango de derecho autónomo y dotándola de una autoridad de control con facultades sancionatorias y de vigilancia.

b) Se determinó que la LOPDP, al incorporar la regulación de la transferencia y comunicación de datos a nivel internacional, sienta las bases para la gestión de los flujos transfronterizos. Sin embargo, este marco inicial resulta insuficiente en su precisión técnica, lo que prefigura la problemática central de la investigación, pues adopta conceptos sin la debida delimitación que exige la complejidad del ecosistema digital global.

c) El análisis de los principios y derechos rectores en este capítulo inicial subraya la importancia del rigor conceptual en el derecho digital, revelando que la omisión en la definición precisa de las figuras de "transferencia" y "comunicación" en el ámbito internacional afectará directamente la capacidad del Estado para garantizar la continuidad de la protección de los datos que salen del país.

2.2. Conclusión del Capítulo II

a) La investigación confirma que la problemática principal del marco ecuatoriano reside en la ambigüedad e indistinción terminológica con que la Ley Orgánica de

Protección de datos Personales aborda las figuras de comunicación internacional y transferencia internacional de datos, esta falta de precisión en los Capítulos V y IX de la ley, genera un vacío de seguridad jurídica que impide a los responsables de tratamiento discernir claramente sus obligaciones y las consecuencias de su incumplimiento, comprometiendo la coherencia interna de la ley.

b) Se concluye que la legislación ecuatoriana es deficiente al no especificar en el cuerpo normativo de la Ley los criterios objetivos y rigurosos que debe emplear la Superintendencia de Protección de Datos Personales para declarar un nivel adecuado de protección de un tercer país; y, al delegar esta esta facultad esencial al reglamento de la Ley, se disminuye el blindaje legal de la decisión y se introduce una incertidumbre sobre la obligación de evaluar los riesgos de vigilancia masiva o desproporcionada, aspecto crucial exigido por el derecho internacional.

c) Se establece que, en su redacción actual, la Ley no proporciona suficientes herramientas para asegurar que los derechos de los titulares se mantengan intactos cuando sus datos son tratados en jurisdicciones extranjeras, lo cual hace necesaria la implementación de mecanismos preventivos y de evaluación de impacto para alinear la normativa nacional con los estándares más exigentes de la protección transfronteriza de datos.

2.3. Conclusión del Capítulo III

a) La revisión del Derecho Comparado, específicamente del Reglamento General de Protección de Datos respecto al flujo de datos, valida la hipótesis de la investigación, la diferenciación técnica entre comunicación y transferencia es indispensable para la aplicación efectiva de los principios de protección, se confirma que los sistemas legales avanzados exigen rigurosas evaluaciones de riesgo para garantizar la continuidad de la protección de los datos transferidos.

b) La propuesta de reforma planteada por este trabajo es técnicamente coherente y

jurídicamente viable para subsanar los vacíos de la Ley, introduciendo definiciones claras y la obligatoriedad de un proceso de evaluación de impacto de las transferencias, el marco legal ecuatoriano podrá gestionar los flujos de datos con un riesgo significativamente menor de vulneración de derechos, dotando de seguridad jurídica tanto a la Autoridad de Control como a los actores económicos.

c) La adopción de una propuesta no solo resuelve un problema normativo interno, sino que fortalece la posición del Ecuador a nivel internacional, al alinearse con los más altos estándares de protección de datos, el país facilita la interoperabilidad y la confianza en los negocios digitales, demostrando un compromiso serio con la defensa de los derechos fundamentales de sus ciudadanos en la economía global del dato.

3. Recomendaciones para el legislador y la Autoridad de Control

3.1. Recomendaciones para el legislador

El análisis de la LOPDP y su Reglamento evidencia vacíos conceptuales y tensiones normativas que generan inseguridad jurídica en la aplicación de las figuras de transferencia y comunicación internacional de datos personales. En línea con lo planteado por Kuner (2013), la falta de definiciones claras sobre flujos transfronterizos provoca interpretaciones divergentes y obstaculiza el cumplimiento efectivo. Por ello, resulta indispensable que el legislador reforme la Ley para incorporar una distinción precisa y operativa entre ambas figuras, estableciendo criterios sobre continuidad del tratamiento, cambio de responsable y tratamiento mediante acceso remoto.

Asimismo, el legislador debe incluir expresamente la obligatoriedad de realizar Evaluaciones de Impacto de Transferencia (TIA) dentro del articulado de la LOPDP. La experiencia europea posterior al caso Schrems II ha demostrado —como sostiene González Fuster (2016)— que los contratos por sí solos no garantizan un nivel de protección adecuado si no se evalúan los riesgos inherentes al país de destino, incluidas

normativas de vigilancia estatal, acceso gubernamental a la información y medidas técnicas disponibles. Pearce y Ausloos (2018) refuerzan esta conclusión al señalar que la evaluación previa de riesgo es la única forma de preservar la “equivalencia esencial” exigida por los estándares modernos de protección.

Por otra parte, el régimen sancionatorio requiere una actualización estructural. Las sanciones deben ser proporcionales y verdaderamente disuasorias para evitar que el incumplimiento resulte más rentable que la observancia. En el contexto ecuatoriano, las multas actuales no representan una carga significativa para grandes empresas ni para proveedores tecnológicos extranjeros. Se recomienda, basado en el modelo brasileño (LGPD), establecer sanciones de entre el 2% al 3% del volumen de negocios para las infracciones muy graves ligadas a transferencias ilegítimas o falta de notificación de incidentes, superando el límite actual del 1% para garantizar la disuasión transnacional.

Del mismo modo, es necesario garantizar la independencia plena de la Autoridad de Control, tal como destacan De Hert y Papakonstantinou (2012), quienes señalan que la autonomía institucional es un requisito esencial para cualquier sistema de supervisión confiable. Ello implica asegurar un proceso de designación técnico, evitar la influencia del poder político y dotar a la institución de un presupuesto estable y suficiente, la meta debe ser alcanzar la autonomía plena de órganos como el INAI de México.

Finalmente, el legislador debe incorporar en la LOPDP criterios mínimos y de rango legal para determinar el “nivel adecuado de protección”. Dejar estos parámetros únicamente en normas reglamentarias reduce la estabilidad del sistema y genera riesgo de cambios abruptos. Por ello, la Ley debe establecer parámetros claros que incluyan garantías constitucionales, mecanismos de control judicial, restricciones a la vigilancia estatal y exigencias de seguridad técnica.

3.2. Recomendaciones para la Autoridad de Control

En el ámbito administrativo, la Autoridad de Control debe fortalecer sus funciones mediante la emisión de lineamientos técnicos vinculantes sobre los mecanismos de transferencia internacional. De acuerdo con Kuner (2020), la existencia de guías interpretativas homogéneas reduce la dispersión de criterios y facilita el cumplimiento, especialmente en jurisdicciones con marcos regulatorios recientes. Esto implica aclarar el uso de cláusulas contractuales tipo, normas corporativas vinculantes, medidas suplementarias y requisitos de las evaluaciones de impacto.

Además, la Autoridad debe mantener un listado público, actualizado y motivado de países con nivel adecuado de protección, sustentado en informes técnicos transparentes. Bygrave (2021) enfatiza que la publicidad de estos listados contribuye a fortalecer la certeza jurídica necesaria para la cooperación digital y para la actividad económica transfronteriza.

En cuanto a la supervisión, la Autoridad debe implementar auditorías periódicas en sectores de alto riesgo como el financiero, salud, educación, telecomunicaciones y servicios digitales, exigiendo evidencia técnica de cumplimiento, contratos de transferencia y matrices de riesgo.

Finalmente, la Autoridad debe crear un sistema nacional de reporte de incidentes de seguridad, interoperable y accesible, que permita notificaciones rápidas y estadísticas anonimizadas. Según De Hert (2020), los sistemas de reporte centralizado fortalecen la capacidad estatal para prevenir vulneraciones, identificar patrones y priorizar acciones de control.

4. Contribuciones de la investigación

La presente investigación realiza aportes relevantes tanto en el plano teórico como en el normativo y práctico del derecho a la protección de datos personales en el Ecuador.

En primer lugar, el trabajo contribuye a la clarificación conceptual del régimen jurídico ecuatoriano al analizar de manera sistemática las diferencias entre las figuras de

transferencia internacional y comunicación internacional de datos personales, identificando sus implicaciones jurídicas, responsabilidades y efectos dentro del tratamiento de datos. Este aporte resulta significativo en un contexto normativo que actualmente presenta ambigüedades interpretativas.

En segundo lugar, la investigación aporta al desarrollo doctrinario nacional, al vincular el derecho a la protección de datos personales con su fundamento constitucional, la jurisprudencia de la Corte Constitucional del Ecuador y los estándares internacionales en materia de autodeterminación informativa, fortaleciendo la comprensión del tratamiento de datos como una actividad jurídicamente regulada y no meramente técnica.

En tercer lugar, el estudio ofrece una contribución normativa concreta, al proponer una reforma articulada a los Capítulos V y IX de la LOPDP, orientada a corregir las contradicciones existentes y a mejorar la coherencia interna del texto legal. Esta propuesta no se limita a una crítica teórica, sino que plantea soluciones específicas y viables dentro del ordenamiento jurídico ecuatoriano.

Adicionalmente, la investigación aporta una guía de factores y un procedimiento metodológico que puede ser utilizado por la Autoridad de Protección de Datos Personales para evaluar y determinar el nivel adecuado de protección de países y empresas receptoras de datos personales. Este aporte tiene un valor práctico directo, al facilitar procesos de autorización más transparentes, objetivos y alineados con el principio de responsabilidad proactiva.

Finalmente, el trabajo contribuye al proceso de armonización del derecho ecuatoriano con los estándares internacionales, promoviendo un modelo de protección de datos personales que permita el flujo transfronterizo de información sin sacrificar los derechos fundamentales de los titulares, fortaleciendo así la confianza jurídica y la competitividad del país en entornos digitales globalizados.

BIBLIOGRAFÍA:

- Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial 449.
- Asamblea Nacional del Ecuador. (2021, 26 de mayo). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459.
- Unión Europea. (2016, 27 de abril). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos - RGPD). Diario Oficial de la Unión Europea L 119/1.
- Presidencia de la República. (2023, 13 de noviembre). Reglamento de Ley Orgánica de Protección de Datos Personales. Tercer Suplemento del Registro Oficial No. 435.
- Asamblea Nacional del Ecuador. (2022, 22 de diciembre). Ley Orgánica Para El Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos. Segundo Suplemento del Registro Oficial No. 215.
- ACTECIL. (s.f.). Transferencia internacional de datos. ACTECIL. Recuperado de Transferencia internacional de datos: ¿qué es y cómo hacerla? - Actecil.
- GDPR-Text.com. (s.f.). Article 44: General principle for transfers. Recuperado de https://gdpr-text.com/read/article-44/
- Marelli, M. (2024). Transferring personal data to international organizations under the GDPR: An analysis of the transfer mechanisms. International Data Privacy Law, 14(1), 19–36. https://doi.org/10.1093/idpl/ipad022
- Jurcys, P., Corrales Compagnucci, M., & Fenwick, M. (2024). The future of international data transfers: Managing legal risk with a user-held data model. Computer Law & Security Review, 46, 105691. https://arxiv.org/abs/2407.20514?utm_source=chatgpt.com.

- Library of Congress. (2024, 13 de mayo). China: New rules on cross-border data transfers released. Global Legal Monitor. https://www.loc.gov/item/global-legal-monitor/2024-05-13/china-new-rules-on-cross-border-data-transfers-released/
- Library of Congress. (2011, 7 de febrero). European Union: Proposed directive on airlines passenger data transfer. Global Legal Monitor. https://www.loc.gov/item/global-legal-monitor/2011-02-07/european-union-proposed-directive-on-airlines-passenger-data-transfer/
- Organización para la Cooperación y el Desarrollo Económico. (1980). “Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.” Organización de los Estados Americanos (OEA). http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf
- Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento N.º 459 de 26 de mayo de 2021. https://www.registrooficial.gob.ec
- Bertoni, E. (2018). Habeas Data y protección de datos personales en América Latina. Universidad de Palermo.
- Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento N.º 459 de 26 de mayo de 2021. https://www.registrooficial.gob.ec
- Solove, D. J. (2021). Understanding Privacy. Harvard University Press
- Bertoni, E. (2018). Derecho a la protección de datos personales: Estándares internacionales y desafíos regionales. Red Iberoamericana de Protección de Datos.
- Bygrave, L. A. (2021). Data Privacy Law: An International Perspective. Oxford University Press.
- Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford University Press.

- OCDE. (2022). Digital Economy Outlook 2022. OECD Publishing. https://doi.org/10.1787/85251b81-en
- Piñar Mañas, J. L. (2018). Tratado de protección de datos personales. Aranzadi.
- Solove, D. J. (2021). Understanding Privacy in the Digital Age. Harvard University Press.
- Tribunal de Justicia de la Unión Europea. (2020). Sentencia de 16 de julio de 2020, Data Protection Commissioner vs. Facebook Ireland y Maximillian Schrems (Schrems II), C-311/18. https://curia.europa.eu
- Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos).
- Consejo de Europa. (2018). Convenio 108+: Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, versión modernizada.
- Departamento de Comercio de los Estados Unidos. (2023). EU–US Data Privacy Framework. https://www.dataprivacyframework.gov
- Agencia Española de Protección de Datos. (2020). Guía para las transferencias internacionales de datos. https://www.aepd.es/es/documento/transferencias-internacionales.pdf
- Comisión Europea. (2021). Transferencia internacional de datos. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_es
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Cámara de Diputados del H. Congreso de la Unión (2010). http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

- Organización para la Cooperación y el Desarrollo Económicos. (2013). Directrices sobre protección de la privacidad y flujos transfronterizos de datos. https://www.oecd.org/sti/ieconomy/oecdprivacyguidelines.htm
- Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, L 119/1. http://data.europa.eu/eli/reg/2016/679/oj
- Comité Europeo de Protección de Datos. (2021). Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers. https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_202105_international_transfers_en.pdf
- González Fuster, G. (2014). The emergence of personal data protection as a fundamental right of the EU. Springer. https://link.springer.com/book/10.1007/978-3-319-05023-2
- Kuner, C. (2020). Transborder data flows and data privacy law. Oxford University Press. https://global.oup.com/academic/product/transborder-data-flows-and-data-privacy-law-9780198871187
- Organización de los Estados Americanos. (2021). Estándares de la OEA sobre privacidad y protección de datos personales. https://www.oas.org/es/sla/ddi/docs/Publicacion-Estándares_de_la_OEA_sobre_Privacidad_y_Protección_de_Datos_Personales.pdf
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). (2016). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Bertoni, E. (2018). Protección de datos personales y autodeterminación informativa. Buenos Aires: CELE.
- CEPD – Comité Europeo de Protección de Datos. (2021). Guidelines on international data transfers. Bruselas.
- Garrido, M. (2020). Derecho a la protección de datos y responsabilidades internacionales. Madrid: Reus.
- Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press.
- OCDE (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. París.