



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

“La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales”

AUTORES:

Johanna Mariuxi Aguilar Espinales

Alexandra Marisela Morán Perero

**Trabajo de titulación previo a la obtención del título de
ABOGADO**

TUTORA:

AB. María Paula Ramírez Vera

GUAYAQUIL, ECUADOR

2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por Johanna Mariuxi Aguilar Espinales y Alexandra Marisela Morán Perero, como requerimiento para la obtención del título de Abogado.

TUTOR

f. _____
AB. MARÍA PAULA RAMÍREZ VERA
DIRECTORA DE LA CARRERA

f. _____
Dra. NURIA PEREZ PUIG-MIR, PHD

Guayaquil, a los 23 del mes de agosto del año 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, Johanna Mariuxi Aguilar Espinales y Alexandra Marisela Morán Perero.

DECLARAMOS QUE:

El Trabajo de Titulación, “La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales” previo a la obtención del título de Abogada, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente, este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. _____
Johanna Mariuxi Aguilar Espinales.

f. _____
Alexandra Marisela Morán Perero



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO

AUTORIZACIÓN

Nosotras, Johanna Mariuxi Aguilar Espinales; y Alexandra Marisela Morán Perero.

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, “La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales”, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. _____

Johanna Mariuxi Aguilar Espinales.

f. _____

Alexandra Marisela Morán Perero



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO



LOS AUTORES

f. _____
Johana Mariuxi Aguilar Espinales

f. _____
Alexandra Marisela Morán Perero

f. _____
ABG. MARIA PAULA RAMIREZ VERA
DOCENTE TUTOR

AGRADECIMIENTO

En primer lugar, agradezco a Dios por darme la fortaleza, la salud y la sabiduría necesarias para llegar hasta este momento y continuar aun en los días difíciles.

Agradezco profundamente a mi familia por su apoyo, comprensión y paciencia durante este camino. También agradezco a mis docentes y tutores por sus conocimientos, orientación y contribución a mi formación profesional.

A mis amigos y a todas las personas que me acompañaron y alentaron durante este proceso, gracias por estar presentes. Finalmente, me agradezco a mí misma por no haberme rendido ante el cansancio, las dificultades y las responsabilidades.

DEDICATORIA

Dedicamos este logro, en primer lugar, a Dios, por darnos la fortaleza, sabiduría y perseverancia necesarias para alcanzar esta meta.

A nuestros hijos e hijas, por ser una de las razones más importantes para seguir adelante. Este logro también es de ustedes y esperamos que les enseñe que, con fe, esfuerzo y perseverancia, los sueños pueden hacerse realidad.

A nuestras familias, padres, abuelos y seres queridos, por su paciencia, compañía, enseñanzas y apoyo durante estos años. Cada experiencia compartida forma parte de las profesionales en las que nos hemos convertido.

A las personas especiales que nos brindaron amistad, palabras de aliento y apoyo sincero, gracias por creer en nosotras. Finalmente, nos dedicamos este logro a nosotras mismas por no habernos rendido y por demostrar que siempre vale la pena luchar por aquello que se desea.



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO

f. _____
AB. MARIA PAULA RAMIREZ VERA —
TUTOR

f. _____
AB. Ángela Paredes Caveró —
COORDINADORA UTE DERECHO

f. _____
Dr. XAVIER ZAVALA EGAS —
DECANO

Facultad: Jurisprudencia y Ciencias Sociales y Políticas

Carrera: Derecho

Período: Semestre A - 2026

Fecha: 23 de agosto del 2026

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado “La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales”, elaborado por los estudiantes Johanna Mariuxi Aguilar Espinales y Alexandra Marisela Morán Perero, certifica que durante el proceso de acompañamiento dichas estudiantes han obtenido la calificación de 7/10, lo cual las califica como **APTAS PARA LA SUSTENTACIÓN.**

f. _____

ABG. María Paula Ramírez Vera

DOCENTE TUTOR

ÍNDICE

INTRODUCCIÓN.....	2
OBJETIVOS DE LA INVESTIGACIÓN	3
Objetivo general	3
Objetivos específicos	3
CAPÍTULO I.....	4
Problema jurídico y antecedentes	4
1. Planteamiento del problema	4
Definición de uso indebido.....	4
Pregunta central de investigación	5
2. Antecedentes históricos y normativos	5
3. Contexto actual en Ecuador.....	5
4. Causas de la vulneración	6
5. Consecuencias jurídicas y sociales	6
6. Sustentación doctrinal	6
7. Análisis crítico del problema jurídico	7
8. Propuesta de solución jurídica.....	8
CAPÍTULO II	9
Marco Teórico y Contextual de la Protección de Datos Personales en Ecuador.....	9
1. Evolución histórica del derecho a la protección de datos.....	9
2. Fundamentos constitucionales y legales en Ecuador.....	10
3. Experiencias internacionales comparadas	12
4. Problemáticas actuales en Ecuador	13
5. Dimensión ética y cultural.....	14
6. Propuestas de fortalecimiento institucional	15
7. Vinculación de casos y comparación internacional	16
CONCLUSIONES.....	17
Correspondencia con los objetivos específicos:	18
RECOMENDACIONES	19
1. Fortalecimiento institucional y transparencia de la autoridad de control	19

2. Auditorías obligatorias	19
3. Régimen sancionatorio proporcional y disuasivo.....	19
4. Integración normativa con ciberseguridad.....	19
5. Educación digital ciudadana y cultura empresarial de cumplimiento	19
Reflexión final	20
REFERENCIAS	21

RESUMEN

La presente investigación analiza el régimen jurídico ecuatoriano de protección de datos personales frente al uso indebido de la información por parte de empresas privadas de telecomunicaciones y plataformas digitales. A partir de una metodología cualitativa, basada en el análisis normativo, doctrinal y jurisprudencial, y de una comparación con experiencias internacionales (el Reglamento General de Protección de Datos de la Unión Europea y la Ley General de Protección de Datos de Brasil), el estudio examina el marco constitucional y legal ecuatoriano —incluida la Ley Orgánica de Protección de Datos Personales (2021)— y su aplicación práctica, evidenciada en casos como Novaestrat (2019) y Worldcoin (2024). Los resultados muestran que, si bien Ecuador cuenta con un marco normativo formalmente sólido, su aplicación es débil debido a la falta de autonomía de la autoridad de control y a la insuficiencia del régimen sancionatorio. La investigación concluye con una propuesta de cinco recomendaciones priorizadas —fortalecimiento institucional, régimen sancionatorio proporcional, auditorías obligatorias, integración con la ciberseguridad, y educación digital ciudadana— orientadas a fortalecer la protección efectiva de los datos personales en el país.

Palabras clave: protección de datos personales, Ley Orgánica de Protección de Datos Personales, telecomunicaciones, plataformas digitales, hábeas data, Ecuador

ABSTRACT

This research analyzes the Ecuadorian legal framework for the protection of personal data against its misuse by private telecommunications companies and digital platforms. Using a qualitative methodology based on the analysis of legislation, legal doctrine, and case law, and a comparison with international experiences (the European Union's General Data Protection Regulation and Brazil's General Data Protection Law), the study examines Ecuador's constitutional and legal framework—including the Organic Law on Personal Data Protection (2021)—and its practical application, as evidenced by cases such as Novaestrat (2019) and Worldcoin (2024). The results show that, although Ecuador has a formally solid regulatory framework, its enforcement remains weak due to the lack of autonomy of the control authority and the insufficiency of the sanctioning regime. The research concludes with five prioritized recommendations—institutional strengthening, proportional sanctions, mandatory audits, integration with cybersecurity, and digital citizen education—aimed at strengthening the effective protection of personal data in the country.

Keywords: personal data protection, Organic Law on Personal Data Protection, telecommunications, digital platforms, habeas data, Ecuador

INTRODUCCIÓN

La protección de los datos personales es uno de los principales retos jurídicos de la era digital. En un contexto interconectado, donde redes sociales, plataformas digitales y servicios de telecomunicaciones gestionan información sensible, los datos personales se han convertido en un recurso estratégico de gran valor económico y social.

En Ecuador, este derecho está reconocido en la Constitución de 2008 (art. 66.19 y art. 92) y desarrollado en la Ley Orgánica de Protección de Datos Personales (2021), que creó la Superintendencia de Protección de Datos Personales. Sin embargo, la práctica evidencia vulneraciones frecuentes, especialmente en telecomunicaciones y plataformas digitales, donde se manejan datos biométricos, financieros y de consumo. Casos como Novaestrat (2019) y Worldcoin (2024) revelan la debilidad institucional y la insuficiencia del régimen sancionatorio.

A nivel internacional, experiencias como el Reglamento General de Protección de Datos (UE, 2016) y la Ley General de Protección de Datos de Brasil (2018) muestran que la protección efectiva requiere sanciones severas, autoridades autónomas y mecanismos tecnológicos de control. En comparación, Ecuador presenta debilidades estructurales que generan un escenario de impunidad y desconfianza ciudadana.

La investigación se justifica porque busca analizar críticamente estas falencias y proponer soluciones normativas e institucionales. Se adopta una metodología cualitativa basada en análisis normativo, doctrinal y jurisprudencial, complementada con comparación internacional. El estudio se inscribe en el campo del derecho constitucional y del derecho de la competencia, vinculado además con la ciberseguridad.

La relevancia social es evidente: la vulneración de datos afecta la privacidad, la seguridad digital y la confianza en las instituciones. Por ello, se plantean propuestas como: autonomía real de la autoridad de control, auditorías obligatorias, sanciones proporcionales, integración normativa

con la ciberseguridad y educación digital ciudadana.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo general

Determinar si el marco jurídico e institucional ecuatoriano es suficiente para prevenir, controlar y sancionar el uso indebido de datos personales por parte de empresas privadas de telecomunicaciones y plataformas digitales, con el propósito de formular lineamientos normativos e institucionales que fortalezcan su aplicación efectiva.

Objetivos específicos

Examinar el marco constitucional, legal y jurisprudencial ecuatoriano en materia de protección de datos personales, así como los antecedentes y el contexto de vulneración evidenciado en los casos Novaestrat y Worldcoin.

Contrastar el tratamiento normativo e institucional ecuatoriano con experiencias internacionales de referencia, en particular el Reglamento General de Protección de Datos de la Unión Europea (RGPD) y la Ley General de Protección de Datos de Brasil (LGPD), identificando prácticas aplicables al contexto nacional.

Determinar las causas estructurales, institucionales y regulatorias, así como las consecuencias jurídicas y sociales, de la vulneración de datos personales por parte de empresas privadas de telecomunicaciones y plataformas digitales en Ecuador.

Formular propuestas normativas e institucionales dirigidas a fortalecer la autonomía de la autoridad de control, el régimen sancionatorio y los mecanismos de cumplimiento empresarial en materia de protección de datos personales.

CAPÍTULO I

Problema jurídico y antecedentes

1. Planteamiento del problema

La protección de los datos personales en Ecuador enfrenta serias limitaciones en su aplicación práctica. Aunque la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales (2021) reconocen este derecho, las vulneraciones son constantes y la institucionalidad encargada de garantizarlo carece de recursos y autonomía.

En la práctica, los ciudadanos se encuentran expuestos a la recopilación, almacenamiento y uso indebido de su información por parte de empresas privadas de telecomunicaciones y plataformas digitales. Estas compañías manejan datos sensibles como números telefónicos, direcciones, historiales de consumo, datos biométricos y financieros, que son utilizados para fines comerciales, publicitarios e incluso de manipulación social.

La ausencia de sanciones proporcionales y la debilidad institucional generan un escenario de impunidad, donde las empresas pueden vulnerar derechos sin enfrentar consecuencias significativas. Este problema jurídico se agrava por la falta de cultura ciudadana en torno a la protección de datos y por la escasa conciencia empresarial sobre la importancia del cumplimiento normativo.

Definición de uso indebido

Para efectos de esta investigación, se entenderá por uso indebido de datos personales todo tratamiento realizado sin consentimiento informado, con fines distintos a los autorizados, sin transparencia respecto de la finalidad, o en contravención de los principios de licitud, proporcionalidad, finalidad y seguridad establecidos en la LOPDP (2021).

Pregunta central de investigación

¿Es suficiente el marco jurídico e institucional vigente en Ecuador para prevenir, controlar y sancionar de manera efectiva el uso indebido de datos personales por parte de empresas privadas de telecomunicaciones y plataformas digitales?

2. Antecedentes históricos y normativos

La evolución de la protección de datos en Ecuador puede dividirse en tres etapas:

- **Etapla inicial (años 90 – 2008):** La protección de datos se vinculaba únicamente al derecho a la intimidad. No existía un reconocimiento explícito de este derecho como autónomo.
- **Etapla constitucional (2008):** La Constitución reconoce expresamente la protección de datos personales en el artículo 66 numeral 19 y establece la acción de hábeas data en el artículo 92.
- **Etapla normativa (2014 – 2021):** El Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014) tipifica delitos informáticos relacionados con el acceso indebido y la divulgación de datos (arts. 229–232). En 2021 se aprueba la Ley Orgánica de Protección de Datos Personales, que crea la Autoridad de Protección de Datos Personales (hoy Superintendencia de Protección de Datos Personales) y establece principios de licitud, transparencia, finalidad, proporcionalidad y seguridad.

3. Contexto actual en Ecuador

El caso Novaestrat (Primicias, 2019) reveló la filtración de datos de más de 17 millones de ecuatorianos, incluyendo información financiera, laboral y de salud. Este hecho evidenció la vulnerabilidad institucional y la ausencia de mecanismos de control. La respuesta estatal fue tardía y limitada, lo que generó desconfianza ciudadana.

El caso Worldcoin (Ecuavisa, 2024) puso en debate la recolección de datos biométricos mediante escaneo de iris. Aunque la empresa ofrecía beneficios económicos a los participantes, la falta de regulación sobre el tratamiento de datos biométricos generó preocupación en la sociedad y en organismos de control.

4. Causas de la vulneración

- Avance acelerado de la economía digital.
- Débil capacidad institucional.
- Falta de sanciones efectivas.
- Escasa cultura empresarial de cumplimiento.
- Ausencia de educación ciudadana sobre el valor de los datos personales.

5. Consecuencias jurídicas y sociales

- Vulneración de la privacidad y seguridad digital.
- Riesgo de manipulación social y política.
- Pérdida de confianza ciudadana en las instituciones.
- Debilitamiento del Estado de derecho.
- Exposición de datos sensibles que pueden ser utilizados para fraudes financieros o suplantación de identidad.

6. Sustentación doctrinal

- Rodotà (2006) relaciona la protección de los datos personales con la dignidad de la persona y con la necesidad de establecer límites jurídicos al tratamiento de la información.

- Díez-Picazo (2005) permite comprender que la protección de la intimidad debe analizarse frente a los nuevos riesgos derivados del desarrollo tecnológico.
- De Hert y Gutwirth (2006) analizan la protección de datos como una garantía vinculada al control que las personas pueden ejercer sobre el uso de su información.
- Westin (1967) concibe la privacidad como una forma de control de la persona sobre la información que decide compartir.
- Solove (2008) advierte que los problemas contemporáneos de privacidad comprenden, entre otros aspectos, la vigilancia, la recopilación y el uso de información personal.

Desde la doctrina latinoamericana, Ordóñez Pineda (2017) sostiene que, en los países de la Comunidad Andina —incluido Ecuador—, la protección de datos personales evolucionó desde una comprensión inicial ligada al derecho a la intimidad hacia su reconocimiento como derecho fundamental autónomo, proceso que en la región se vincula estrechamente con la necesidad de proteger a los ciudadanos frente al poder de las empresas privadas y no únicamente frente al Estado, lo que resulta directamente pertinente para el problema jurídico examinado en esta investigación.

7. Análisis crítico del problema jurídico

El principal problema jurídico radica en la contradicción entre el reconocimiento constitucional del derecho a la protección de datos y su débil aplicación práctica. La Superintendencia de Protección de Datos Personales carece de autonomía administrativa y financiera, lo que limita su capacidad de control y fiscalización.

Las sanciones previstas en la LOPDP resultan insuficientes frente al poder económico de las grandes corporaciones, generando un escenario de impunidad. A esto se suma la escasa cultura

empresarial de cumplimiento, que provoca prácticas laxas en el manejo de información y mínima inversión en seguridad digital.

La debilidad en los mecanismos de denuncia y acceso a la justicia agrava la situación: los procesos son largos y poco efectivos, y la falta de jueces especializados limita la protección real de los ciudadanos. Finalmente, la ausencia de coordinación entre la autoridad de datos y otras instituciones estatales evidencia una fragmentación institucional que impide implementar políticas integrales y eficaces.

8. Propuesta de solución jurídica

- **Fortalecimiento institucional:** Autonomía plena de la Superintendencia de Protección de Datos Personales.
- **Auditorías obligatorias:** En empresas privadas que gestionen grandes volúmenes de datos.
- **Régimen sancionatorio severo:** Multas proporcionales y progresivas inspiradas en el RGPD europeo.
- **Integración normativa con ciberseguridad:** Protocolos de respuesta ante incidentes de filtración o robo de información.
- **Educación digital ciudadana:** Campañas de concienciación sobre el valor de los datos personales.
- **Transparencia estatal:** Procesos de fiscalización imparciales y libres de corrupción.

CAPÍTULO II

Marco Teórico y Contextual de la Protección de Datos Personales en Ecuador

1. Evolución histórica del derecho a la protección de datos

La protección de datos personales no surge de manera aislada, sino como resultado de un proceso histórico vinculado al reconocimiento progresivo de los derechos fundamentales. En la segunda mitad del siglo XX, el desarrollo de las tecnologías de la información y la comunicación generó nuevas formas de almacenamiento y tratamiento de información, lo que obligó a los Estados a replantear la noción de privacidad. En Europa, países como Alemania y Francia fueron pioneros en establecer leyes específicas que regulaban el uso de datos personales, sentando las bases para lo que posteriormente sería el Reglamento General de Protección de Datos (RGPD).

En América Latina, el reconocimiento de este derecho fue más tardío, y en muchos casos se vinculó con la necesidad de proteger a los ciudadanos frente al poder de las empresas multinacionales y los Estados. Ecuador, en su Constitución de 2008, dio un paso importante al reconocer la protección de datos como un derecho fundamental, pero la implementación práctica ha sido limitada. La Ley Orgánica de Protección de Datos Personales (2021) constituye un avance significativo, aunque aún enfrenta desafíos en su aplicación.

El desarrollo histórico de este derecho también se relaciona con la evolución de la noción de privacidad en la sociedad. En sus inicios, la privacidad se entendía como el derecho a estar “solo” o a mantener la vida personal fuera del escrutinio público. Sin embargo, con el avance de las tecnologías digitales, la privacidad adquirió una dimensión más compleja, vinculada al control sobre la información personal y a la capacidad de decidir cómo, cuándo y con quién se comparte. Este cambio conceptual fue fundamental para que los Estados reconocieran la necesidad de regular el tratamiento de datos personales como un derecho autónomo.

Asimismo, la evolución histórica demuestra que la protección de datos no puede desvincularse de otros derechos fundamentales, como la libertad de expresión, el derecho a la información y el derecho al honor. En muchos países, los debates sobre protección de datos surgieron precisamente de conflictos entre estos derechos, lo que obligó a los legisladores y jueces a buscar un equilibrio adecuado. En Ecuador, este proceso aún está en construcción, y la experiencia internacional ofrece lecciones valiosas para consolidar un sistema jurídico que garantice la protección efectiva de los datos personales en armonía con otros derechos constitucionales.

2. Fundamentos constitucionales y legales en Ecuador

El marco constitucional ecuatoriano establece que toda persona tiene derecho a la protección de sus datos personales, incluyendo el acceso, rectificación y eliminación de la información que se encuentre en registros públicos o privados. Este reconocimiento se complementa con la acción de hábeas data, que permite a los ciudadanos exigir la corrección o eliminación de información incorrecta o utilizada de manera indebida.

La Ley Orgánica de Protección de Datos Personales desarrolla estos principios y establece obligaciones para las entidades públicas y privadas que manejan información personal. Entre los aspectos más relevantes se encuentran la necesidad de obtener consentimiento informado, la obligación de garantizar la seguridad de los datos y la prohibición de transferir información sin autorización. Sin embargo, aunque la Ley Orgánica de Protección de Datos Personales otorga a la Superintendencia de Protección de Datos Personales competencias de control, vigilancia y potestad sancionadora, persisten desafíos para garantizar la efectividad de estas atribuciones en la práctica. En particular, el artículo 76, numerales 2, 3 y 4, de la LOPDP faculta a la Autoridad para ejercer la potestad sancionadora, conocer, sustanciar y resolver reclamos, incluso aquellos iniciados de oficio, y realizar o delegar auditorías técnicas al tratamiento de datos personales. Por

ello, el problema no se encuentra en la ausencia de competencia legal, sino en determinar si los mecanismos institucionales y normativos disponibles permiten ejercer estas facultades de manera efectiva frente al uso indebido de datos personales por parte de empresas privadas. Un aspecto fundamental del marco legal ecuatoriano es la interconexión con otros derechos constitucionales. La protección de datos personales se vincula directamente con la intimidad, el honor, la reputación y la libertad de expresión. Esto significa que cualquier vulneración en el tratamiento de datos afecta de manera transversal a varios derechos fundamentales, lo que obliga a los jueces y autoridades a interpretar la normativa de manera integral. La acción de hábeas data, en este sentido, se convierte en un mecanismo clave para garantizar la tutela efectiva de los derechos.

En materia jurisprudencial, la Corte Constitucional del Ecuador, mediante la Sentencia No. 2064-14-EP/21 (2021), sentó un precedente relevante sobre el derecho a la protección de datos personales y la autodeterminación informativa, vinculándolo con los derechos a la imagen, la honra y el buen nombre, y reforzando así la garantía constitucional de hábeas data frente al tratamiento indebido de información personal por parte de terceros.

En el plano institucional, el marco normativo ecuatoriano ha tenido desarrollos posteriores a la expedición de la Ley Orgánica de Protección de Datos Personales: en noviembre de 2023 se expidió el Reglamento General a dicha ley mediante el Decreto Ejecutivo No. 904 (Presidencia de la República del Ecuador, 2023), y en agosto de 2024 se conformó la Superintendencia de Protección de Datos Personales, cuya Resolución N° SPDP-SPDP-2024-0001-R estableció su estructura orgánica provisional (Superintendencia de Protección de Datos Personales del Ecuador, 2024). Se trata de avances institucionales relevantes que, sin embargo, se encuentran aún en una fase inicial de consolidación y cuyo desempeño excede el periodo cubierto por el análisis central de este trabajo.

En materia jurisprudencial reciente, la Corte Constitucional del Ecuador, mediante la Sentencia No. 1068-19-JP/25 (2025), fijó estándares vinculantes para las empresas operadoras de telefonía móvil en la verificación de identidad y en la obtención del consentimiento expreso de los usuarios, exigiendo el cruce de información con el Registro Civil y la conservación de los respaldos de contratación. Este precedente resulta directamente aplicable al problema estudiado, pues incide de manera específica sobre el tratamiento de datos personales por parte de empresas privadas de telecomunicaciones.

Asimismo, la normativa ecuatoriana reconoce principios esenciales como la licitud, la proporcionalidad y la finalidad en el tratamiento de datos. Estos principios buscan asegurar que la información personal sea utilizada únicamente para los fines autorizados y que no se recopile más información de la necesaria. Sin embargo, en la práctica, muchas instituciones públicas y privadas no cumplen con estos principios, lo que genera un escenario de vulnerabilidad para los ciudadanos. La falta de auditorías periódicas y de controles efectivos limita la capacidad del Estado para garantizar el cumplimiento real de la ley.

3. Experiencias internacionales comparadas

Asimismo, en materia de vulneraciones de seguridad, el artículo 33 del RGPD establece como regla que la notificación a la autoridad de control debe realizarse, cuando sea posible, dentro de las 72 horas siguientes a que el responsable tenga conocimiento de la vulneración. Este mecanismo permite una intervención temprana de la autoridad frente a incidentes que puedan afectar los derechos de los titulares. Por su parte, la LOPDP establece un mecanismo propio de notificación de vulneraciones de seguridad, por lo que el análisis comparativo permite determinar si los plazos y procedimientos previstos en Ecuador ofrecen una respuesta igualmente oportuna. De igual manera, el artículo 37 del RGPD establece la designación obligatoria de un delegado de

protección de datos en determinados supuestos, entre ellos cuando las actividades principales impliquen una observación habitual y sistemática de interesados a gran escala o el tratamiento a gran escala de categorías especiales de datos. En consecuencia, el contraste con el RGPD permite identificar como punto de análisis la necesidad de fortalecer la capacidad preventiva, de respuesta ante vulneraciones y de disuasión del régimen ecuatoriano, especialmente respecto de empresas privadas que realizan tratamientos masivos de datos personales. Además, reconoce derechos específicos como la portabilidad de datos y el derecho al olvido, que fortalecen la capacidad de los ciudadanos para controlar su información.

En Brasil, la LGPD ha tenido un impacto positivo en la cultura empresarial, obligando a las compañías a implementar políticas de cumplimiento y a designar responsables de protección de datos. En países como España, la existencia de una autoridad independiente con capacidad sancionadora ha permitido consolidar un sistema robusto de protección. Estas experiencias demuestran que la clave no está únicamente en la existencia de normas, sino en la capacidad institucional para aplicarlas de manera efectiva.

4. Problemáticas actuales en Ecuador

También, existe una fragmentación institucional que dificulta la coordinación entre la Superintendencia de Protección de Datos Personales, la Agencia de Regulación de Telecomunicaciones y otras entidades relacionadas con la ciberseguridad. Esta falta de articulación genera vacíos de control y limita la eficacia de las políticas públicas.

Otro problema relevante es la escasa capacitación de los funcionarios públicos y de los responsables de tratamiento de datos en las empresas privadas. La normativa exige el cumplimiento de principios como licitud, proporcionalidad y finalidad, pero en la práctica muchos operadores desconocen cómo aplicarlos correctamente. Esta falta de formación técnica y jurídica

genera errores en el manejo de información y aumenta el riesgo de vulneraciones, lo que evidencia la necesidad de programas de capacitación permanentes y especializados.

La ausencia de mecanismos de supervisión tecnológica adecuados es otro factor determinante: en un contexto donde el uso de inteligencia artificial, big data y plataformas digitales se expande rápidamente, el Estado carece de herramientas modernas para auditar y controlar el tratamiento de datos personales. Esta carencia limita la capacidad de respuesta frente a vulneraciones masivas y coloca a los ciudadanos en una situación de desprotección frente al poder de las corporaciones tecnológicas.

5. Dimensión ética y cultural

La protección de datos no puede reducirse a un aspecto técnico o jurídico, sino que implica valores como la dignidad, la autonomía y el respeto a la persona. En Ecuador, muchos ciudadanos no son conscientes del valor de su información y la comparten sin precaución en redes sociales y plataformas digitales. Esta falta de cultura de protección facilita que las empresas recopilen y utilicen datos sin consentimiento informado. La educación digital se convierte en un pilar indispensable para que la ciudadanía pueda ejercer sus derechos de manera efectiva.

En el plano cultural, la sociedad ecuatoriana enfrenta el reto de construir una conciencia colectiva sobre la importancia de la privacidad digital. La normalización del intercambio indiscriminado de información en redes sociales y plataformas tecnológicas ha debilitado la percepción de riesgo frente a la exposición de datos. Esta situación demanda políticas públicas que promuevan campañas de sensibilización y programas educativos que fortalezcan la cultura de protección de datos. Solo mediante un cambio cultural profundo será posible consolidar un entorno digital seguro, donde los ciudadanos ejerzan sus derechos con responsabilidad y las instituciones actúen con transparencia.

6. Propuestas de fortalecimiento institucional

Un primer eje de fortalecimiento institucional debe centrarse en la independencia de la Superintendencia de Protección de Datos Personales. Mientras esta entidad dependa financieramente del Ejecutivo, su capacidad de fiscalización se verá limitada por presiones políticas y económicas. La autonomía administrativa y presupuestaria permitiría que la autoridad actúe con imparcialidad, garantizando que las decisiones de control y sanción respondan exclusivamente a la protección de los derechos ciudadanos.

Otro aspecto clave es la creación de mecanismos de auditoría obligatoria para las empresas que gestionen grandes volúmenes de información. Estas auditorías deben ser periódicas y realizadas por entidades certificadas, con el fin de verificar el cumplimiento de los principios de licitud, proporcionalidad y seguridad en el tratamiento de datos. La implementación de este sistema no solo fortalecería la confianza ciudadana, sino que también incentivaría a las empresas a invertir en infraestructura tecnológica y protocolos internos de protección.

Por otra parte, resulta indispensable consolidar una política pública integral que articule a la Superintendencia de Protección de Datos Personales con otras instituciones vinculadas, como la Agencia de Regulación de Telecomunicaciones, la Superintendencia de Bancos y los organismos de ciberseguridad. La coordinación interinstitucional permitiría enfrentar de manera conjunta los riesgos derivados del uso de inteligencia artificial, big data y plataformas digitales, garantizando un control más efectivo y una respuesta rápida frente a vulneraciones masivas.

Finalmente, debe contemplarse la creación de un sistema de rendición de cuentas ciudadana que permita evaluar periódicamente el desempeño de la Superintendencia de Protección de Datos Personales y de las empresas que manejan información personal. Este mecanismo fortalecería la transparencia institucional y otorgaría a la ciudadanía un rol activo en la vigilancia del

cumplimiento de la normativa, asegurando que la protección de datos no dependa únicamente de la acción estatal, sino también de la participación social.

7. Vinculación de casos y comparación internacional

A. Análisis de los casos Novaestrat y Worldcoin

En el caso Worldcoin, el tratamiento de datos biométricos permite examinar la aplicación práctica de las reglas ecuatorianas sobre consentimiento, finalidad, proporcionalidad, información al titular y seguridad. El caso resulta pertinente para valorar si los mecanismos existentes permiten controlar adecuadamente tratamientos realizados por plataformas digitales.

B. Experiencias internacionales comparadas: RGPD y LGPD

En cuanto al Reglamento General de Protección de Datos (RGPD) de la Unión Europea, se observa que en Europa es obligatorio que ciertas empresas tengan a alguien encargado de vigilar que se cumplan las reglas de protección de datos. Eso ayuda a que no se cometan errores ni abusos desde adentro. En Ecuador no es obligatorio, y eso hace que falte quien cuide que todo se haga bien. Por ejemplo, en el caso de Worldcoin, si hubiera alguien encargado de vigilar el cumplimiento desde dentro, quizás se habrían evitado muchas dudas y riesgos.

CONCLUSIONES

En relación con el primer objetivo específico, el examen del marco constitucional, legal y jurisprudencial ecuatoriano permite concluir que Ecuador cuenta con un reconocimiento normativo formalmente completo de la protección de datos personales —el artículo 66 numeral 19 y el artículo 92 de la Constitución de la República (2008), la Ley Orgánica de Protección de Datos Personales (2021) y el precedente de la Corte Constitucional en la Sentencia No. 2064-14-EP/21 (2021)—, pero cuya aplicación práctica es débil. Los casos Novaestrat (Primicias, 2019) y Worldcoin (Ecuavisa, 2024) evidenciaron, respectivamente, la vulnerabilidad frente a la filtración masiva de información y la ausencia de regulación específica para el tratamiento de datos biométricos por parte de empresas privadas.

En cuanto al segundo objetivo específico, el contraste con el Reglamento General de Protección de Datos de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2016) y la Ley General de Protección de Datos de Brasil (Presidencia de la República Federativa de Brasil, 2018) muestra que la efectividad de un régimen de protección de datos depende, sobre todo, de la autonomía real de la autoridad de control y de la severidad disuasiva de las sanciones. En estos dos aspectos, la institucionalidad ecuatoriana presenta un desarrollo incipiente; la creación de la Superintendencia de Protección de Datos Personales en 2024 (Resolución N° SPDP-SPDP-2024-0001-R) constituye un primer paso en esa dirección, cuyo desempeño deberá evaluarse en investigaciones posteriores.

Respecto al tercer objetivo específico, el análisis realizado permite concluir que la vulneración de datos personales en Ecuador obedece a causas concurrentes —el avance acelerado de la economía digital, la debilidad institucional, la insuficiencia de sanciones y la escasa cultura de cumplimiento— y que sus efectos comprometen de manera directa la protección efectiva de los

titulares frente a empresas de telecomunicaciones y plataformas digitales, generando riesgos de impunidad, pérdida de confianza institucional y afectación a la autodeterminación informativa documentados en el Capítulo II.

Finalmente, en relación con el cuarto objetivo específico, la investigación permite concluir que el fortalecimiento de la protección de datos personales en Ecuador requiere, de manera prioritaria, la autonomía administrativa y financiera de la autoridad de control y un régimen sancionatorio proporcional al poder económico de los sujetos obligados. La evidencia comparada analizada (RGPD y LGPD) vincula estas dos medidas de forma más directa con la reducción efectiva de vulneraciones, mientras que las auditorías obligatorias, la integración con la ciberseguridad y la educación digital ciudadana operan como mecanismos complementarios que dependen de la existencia previa de una autoridad con capacidad real de fiscalización.

Correspondencia con los objetivos específicos:

- Objetivo específico 1 (marco jurídico y contexto): reconocimiento normativo sólido, aplicación práctica débil, evidenciada en los casos Novaestrat y Worldcoin.
- Objetivo específico 2 (comparación internacional): la autonomía de la autoridad de control y la severidad sancionatoria son los factores que marcan la diferencia frente al RGPD y la LGPD.
- Objetivo específico 3 (causas y consecuencias): las vulneraciones responden a causas estructurales, institucionales y regulatorias interconectadas, con riesgo de impunidad, pérdida de confianza institucional y afectación a la autodeterminación informativa de los titulares.
- Objetivo específico 4 (propuestas): la autonomía institucional y el régimen sancionatorio son las medidas prioritarias; las demás operan como mecanismos complementarios.

RECOMENDACIONES

La investigación evidenció debilidades estructurales concretas en la protección de datos personales en Ecuador. Por ello, y en atención al criterio de que las recomendaciones deben desprenderse directamente de los hallazgos, se plantean cinco recomendaciones prioritarias, concretas, jurídicamente viables y justificadas en los resultados de la investigación.

1. Fortalecimiento institucional y transparencia de la autoridad de control

Garantizar autonomía administrativa, financiera y técnica de la Superintendencia de Protección de Datos Personales, con transparencia y rendición de cuentas.

2. Auditorías obligatorias

Implementar controles periódicos en empresas que gestionen grandes volúmenes de datos, para verificar cumplimiento normativo y seguridad digital.

3. Régimen sancionatorio proporcional y disuasivo

Ajustar las multas para que sean disuasivas frente al poder económico de las corporaciones, tomando como referencia el RGPD europeo.

4. Integración normativa con ciberseguridad

Vincular la protección de datos con políticas de ciberseguridad, estableciendo protocolos técnicos de prevención y respuesta ante vulneraciones.

5. Educación digital ciudadana y cultura empresarial de cumplimiento

Promover campañas de sensibilización y cultura empresarial de cumplimiento, fortaleciendo el conocimiento ciudadano sobre el valor de sus datos.

Reflexión final

Las cinco recomendaciones planteadas no deben entenderse como medidas aisladas, sino como una estrategia priorizada a partir de los hallazgos de la investigación: el fortalecimiento institucional y la transparencia de la autoridad de control, un régimen sancionatorio proporcional y disuasivo, auditorías obligatorias, la integración con la ciberseguridad, y la educación digital ciudadana junto con el cumplimiento empresarial.

La aplicación de estas recomendaciones requiere voluntad política, compromiso empresarial y conciencia ciudadana. Solo mediante un esfuerzo conjunto será posible que la protección de datos personales deje de ser un principio enunciado en la normativa y se convierta en una realidad efectiva que fortalezca la democracia, la confianza institucional y la dignidad humana en la era digital.

REFERENCIAS

- Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449, 20 de octubre de 2008.
- Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal (COIP)*. Registro Oficial Suplemento 180, 10 de febrero de 2014.
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459, 26 de mayo de 2021.
- Corte Constitucional del Ecuador. (2021). *Sentencia No. 2064-14-EP/21*. <https://www.corteconstitucional.gob.ec/sentencia-2064-14-ep-21/>
- Corte Constitucional del Ecuador. (2025). *Sentencia No. 1068-19-JP/25*, de 6 de febrero de 2025. <https://www.dpe.gob.ec/sentencia-caso-1068-19-jp-25/>
- De Hert, P., & Gutwirth, S. (2006). Privacy, data protection, and law enforcement. Opacity of the individual and transparency of power. En E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 61–104). Intersentia.
- Díez-Picazo, L. M. (2005). *Sistema de derechos fundamentales* (2.a ed.). Civitas.
- Ecuavisa. (2024, 1 de agosto). *Worldcoin en Ecuador: ¿Cuáles son los riesgos y cómo se puede usar la información obtenida del escaneo del iris?* <https://www.ecuavisa.com/noticias/seguridad/2024-08-01-worldcoin-ecuador-escaneo-iris-DD7775371>
- Ordóñez Pineda, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. *Foro, Revista de Derecho*, (27), 83–114. <https://www.redalyc.org/pdf/900/90075911005.pdf>

- Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 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 (*RGPD*). Diario Oficial de la Unión Europea, L119. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>
- Presidencia de la República del Ecuador. (2023). Decreto Ejecutivo No. 904: Reglamento General a la Ley Orgánica de Protección de Datos Personales, de 6 de noviembre de 2023.
- Presidencia de la República Federativa de Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (*LGPD*), Lei n.º 13.709.
- Primicias. (2019, 16 de septiembre). *Datos de 17 millones de ecuatorianos fueron filtrados*. <https://www.primicias.ec/noticias/tecnologia/datos-17-millones-ecuatorianos-fueron-filtrados/>
- Rodotà, S. (2006). *La vita e le regole. Tra diritto e non diritto*. Feltrinelli.
- Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
- Superintendencia de Protección de Datos Personales del Ecuador. (2024). Resolución N° SPDP-SPDP-2024-0001-R, de 19 de agosto de 2024, que establece la estructura orgánica provisional de la Superintendencia. <https://www.gob.ec/spdp>
- Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

DECLARACIÓN Y AUTORIZACIÓN

Nosotras, Johanna Mariuxi Aguilar Espinales, con C.I. 0957757602, y Alexandra Marisela Morán Perero, con C.I. 0924030638, respectivamente, autoras del trabajo de titulación: “La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales”, previo a la obtención del título de Abogado en la Universidad Católica de Santiago de Guayaquil:

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 23 de agosto de 2026

f. _____

Johanna Mariuxi Aguilar Espinales —

C.I: 0957757602

f. _____

Alexandra Marisela Morán Perero —

C.I: 0924030638

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	La protección de los datos personales en el Ecuador frente al uso indebido por parte de empresas privadas de telecomunicaciones y plataformas digitales
AUTOR (ES)	Johanna Mariuxi Aguilar Espinales; Alexandra Marisela Morán Perero
REVISOR(ES)/TUTOR(ES)	Ab. María Paula Ramírez Vera
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas
CARRERA:	Carrera de Derecho
TÍTULO OBTENIDO:	Abogado
FECHA DE PUBLICACIÓN:	Guayaquil, a los 23 del mes de agosto del año 2026
No. DE PÁGINAS:	35
ÁREAS TEMÁTICAS:	Derecho Constitucional; Derecho de las Tecnologías de la Información; Protección de Datos Personales
PALABRAS CLAVES/ KEYWORDS:	Protección de datos personales; Ley Orgánica de Protección de Datos Personales; telecomunicaciones; plataformas digitales; hábeas data; Ecuador
RESUMEN/ABSTRACT:	La presente investigación analiza el régimen jurídico ecuatoriano de protección de datos personales frente al uso indebido de la información por parte de empresas privadas de telecomunicaciones y plataformas digitales. A partir de una metodología cualitativa, basada en el análisis normativo, doctrinal y jurisprudencial, y de una comparación con experiencias internacionales (el Reglamento General de Protección de Datos de la Unión Europea y la Ley General de Protección de Datos de Brasil), el estudio examina el marco constitucional y legal ecuatoriano —incluida la Ley Orgánica de Protección de Datos Personales (2021)— y su aplicación práctica, evidenciada en casos como Novaestrat (2019) y Worldcoin (2024). Los resultados muestran que, si bien Ecuador cuenta con un marco normativo formalmente sólido, su aplicación es débil debido a la falta de autonomía de la autoridad de control y a la insuficiencia del régimen sancionatorio. La investigación concluye con una propuesta de cinco recomendaciones priorizadas —fortalecimiento institucional, régimen sancionatorio proporcional, auditorías obligatorias, integración con la ciberseguridad, y educación digital ciudadana— orientadas a fortalecer la protección efectiva de los datos personales en el país.
ADJUNTO PDF:	SI (X) NO ()
CONTACTO CON AUTOR/ES:	Teléfono: [0993480796 - 0969908128] E-mail: [alexandra.moran01@cu.ucsg.edu.ec] johanna.aguilar02@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	Nombre: Ab. Ángela Paredes Cavero, Mgtr. Teléfono: +593-99 760 4781 E-mail: angela.paredes01@cu.ucsg.edu.ec