UNIVERSIDAD ESTATAL DE BOLÍVAR

Facultad de Jurisprudencia Ciencias Sociales y Políticas

Carrera de Derecho

Trabajo de Integración Curricular Modalidad Proyecto de Investigación
Previo la obtención del Título de Abogada

Tema:

Análisis jurídico de la venta de datos personales por empresas frente al derecho a la protección de datos personales y su regulación vigente

Investigadora:

Mayerlin Alejandra Guzmán Tocto

Tutor del Proyecto de Investigación:

Dra. Karina Marianela Ruiz Abril

Guaranda - Ecuador

2024

CERTIFICACIÓN DE AUTORÍA

Yo, **Doctora Karina Marianela Ruiz Abril** en mi calidad de Tutora del Proyecto de Investigación, designado por disposición de Consejo Directivo, bajo juramento **CERTIFICO:** que la señorita **Mayerlin Alejandra Guzmán Tocto,** egresada de la Universidad Estatal de Bolívar, Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Derecho, ha cumplido con su trabajo de grado previo a la obtención del título de Abogada; con el tema: **"ANÁLISIS JURÍDICO DE LA VENTA DE DATOS PERSONALES POR EMPRESAS FRENTE AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU REGULACIÓN VIGENTE";** mismo que ha cumplido con todos los requerimientos exigidos por la institución, por lo que se aprueba la misma.

Es todo cuanto puedo decir en honor a la verdad, facultando a la interesada a hacer uso de la presente, así como también se autoriza la presentación para la calificación por parte del jurado respectivo.

Atentamente,

Dra. Karina Ruiz Abril

Tutora

DECLARACIÓN JURAMENTADA DE AUTENTICIDAD DE AUTORÍA

Yo; **MAYERLIN ALEJANDRA GUZMÁN TOCTO**, egresada de la Carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, bajo juramento declaro en forma libre y voluntaria que el presente Proyecto, con el tema: **"ANÁLISIS JURÍDICO DE LA VENTA DE DATOS PERSONALES POR EMPRESAS FRENTE AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU REGULACIÓN VIGENTE"**; es de mí autoría, así como las expresiones vertidas en la misma, que se ha realizado bajo la recopilación bibliográfica tanto de libros, revistas, publicaciones, así como de artículos de la legislación ecuatoriana para el presente trabajo investigativo.

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

Atentamente,

Mayerlin Alejandra Guzmán Tocto

Autora

Notaria Tercera del Cantón Guaranda
Msc.Ab. Henry Rojas Narvaez
Notario

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

rio...

N° ESCRITURA 20250201003P00620

DECLARACION JURAMENTADA

OTORGADA POR: **GUZMÁN TOCTO MAYERLIN ALEJANDRA**

INDETERMINADA DI: 2 COPIAS

H.R.

Factura: 001-006- 000007506

En la ciudad de Guaranda, capital de la provincia Bolívar, República del Ecuador, hoy día trece de Marzo del dos mil veinticinco, **ante mi Abogado HENRY ROJAS NARVAEZ, Notario Público Tercero del Cantón Guaranda,** comparece la señorita **GUZMÁN TOCTO MAYERLIN ALEJANDRA**, de estado civil soltera de ocupación estudiante, domiciliada en el cantón Montalvo de la provincia de los Ríos y de paso por este lugar, con celular número (0988220145), su correo electrónico es mayguzman@mailes.ueb.edu.ec , por sus propios y personales derechos, a quien de obligarse y de conocer doy fe en virtud de haberme exhibido sus documentos de identificación y con su autorización se ha procedido a verificar la información en el Sistema Nacional de Identificación Ciudadana; bien instruidas por mí el Notario con el objeto y resultado de esta escritura pública a la que procede libre y voluntariamente, advertido de la gravedad del juramento y las penas de perjurio, me presenta su declaración Bajo Juramento declara lo siguiente manifiesto que el criterio e ideas emitidas en el presente trabajo de investigación titulado **"ANÁLISIS JURÍDICO DE LA VENTA DE DATOS PERSONALES POR EMPRESAS FRENTE AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU REGULACIÓN VIGENTE";** Es de mi exclusiva responsabilidad en calidad de autora, previo a la obtención del título de Abogada de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, Es todo cuanto puedo declarar en honor a la verdad, la misma que la hago para los fines legales pertinentes. HASTA AQUÍ LA DECLARACIÓN JURADA. La misma que elevada a escritura pública con todo su valor legal. Para el otorgamiento de la presente escritura pública se observaron todos los preceptos legales del caso, leída que le fue a la compareciente por mí el Notario en unidad de acto, aquella se ratifica y firma conmigo de todo lo cual doy Fe.

B.0884705

GUZMÁN TOCTO MAYERLIN ALEJANDRA

C.C. 0202327912

AB. HENRY ROJAS NARVAEZ

NOTARIO PUBLICO TERCERO DEL CANTON GUARANDA

EL NOTA....

Certificado de Turnitin

Alejandra Guzman

Informe Final Mayerlin Alejandra Guzmán Tocto.docx

Tesis 2025
Tesis 2025
Universidad Estatal de Bolivar

Detalles del documento

Identificador de la entrega
trn:oid:::3117:439100710

Fecha de entrega
13 mar 2025, 2:21 p.m. GMT-5

Fecha de descarga
13 mar 2025, 3:01 p.m. GMT-5

Nombre de archivo
Informe Final Mayerlin Alejandra Guzmán Tocto.docx

Tamaño de archivo
239.2 KB

70 Páginas

14,727 Palabras

83,324 Caracteres

0% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 108 palabras)

Fuentes principales

0% Fuentes de Internet
0% Publicaciones
0% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dra. Karina Marianela Ruiz Abril
Tutora

DERECHOS DE AUTOR

Yo; Mayerlin Alejandra Guzmán Tocto, portador de la Cédula de Identidad No 0202327912, en calidad de autor titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Análisis jurídico de la venta de datos personales por empresas frente al derecho a la protección de datos personales y su regulación vigente,** Modalidad Proyecto de Investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Mayerlin Alejandra Guzmán Tocto

Autora

DEDICATORIA

A Dios padre celestial por brindarme el don de la vida, a mis amados padres Walter Guzmán y Melany Tocto por ser el pilar fundamental e inspiración constante de cada logro que obtengo en mi vida, ya que con su inmenso amor, fortaleza, bondad y apoyo incondicional soy la persona de bien hoy en día, todo gracias a su ejemplo, este triunfo es por y para ustedes, la razón de mi existir, mi perseverancia y esfuerzo . Agradezco a Dios por haberme escogido como su hija, son lo más bonito y único que tengo en esta vida.

A mis queridos hermanos que la vida me regaló Dania y Adonis que han incentivando día a día a no rendirme y más de una vez han hecho lo imposible para darme aliento a continuar y estar acompañándome en este largo camino y etapa que llega a su final.

A mis amados hijos que son más que mis mascotas, son mi vida y quienes me dan el vigor de vivirla

Alejandra

AGRADECIMIENTO

Mi sincera gratitud a la Universidad Estatal de Bolívar, Alma Mater de la Educación Superior Bolivarense.

Especial reconocimiento merecen los maestros catedráticos que impartieron su sabiduría y conocimientos, en el transcurso de esta larga etapa académica.

A mí queridos amigos/as por más de una vez sacarme una sonrisa cuando más lo he necesito y han hecho de esta una experiencia más amena pese a las dificultades que se nos presentan diariamente, en especial a Leito por ser esa calidad de persona, siempre apoyarme y más de una vez en ayudarme en situaciones que la vida nos dispone y general cada persona que cerca o lejos han sido testigos de este gran esfuerzo, pese a qué hoy por hoy ya no estén inmersos en mi vida

Mayerlin Alejandra Guzmán Tocto

Contenido

CERTIFICACIÓN DE AUTORÍA I

DECLARACIÓN JURAMENTADA DE AUTENTICIDAD DE AUTORÍA II

DEDICATORIA II

AGRADECIMIENTO V

TITULO 1

CAPITULO I 2

1. PROBLEMA 2

1.1. Resumen 2

1.2. Introducción 6

1.3. Planteamiento del Problema 10

1.4. Formulación del Problema 11

1.5. Hipótesis 11

1.6. Variables 11

1.7. Objetivos 12

1.8. Justificación 12

CAPITULO II 15

2. Marco Teórico 15

2.1. 1. Concepto de Datos Personales y su Importancia Jurídica 15

2.1.2. Tipos de Datos Personales 17

2.1.3. Evolución histórica de la legalización de los Datos Personales 21

2.1.4. El Derecho a la Protección de Datos de Carácter Personal 23

2.1.5. Principios Rectores del Tratamiento de Datos Personales 27

2.1.6. La Autodeterminación Informativa 29

2.1.7. Normativa internacional y su influencia en la regulación ecuatoriana 31

2.1.8. La venta de los Datos personales 31

2.1.9. Riesgos asociados a la venta de datos personales 33

2.1.10. Sanciones y responsabilidades 35
CAPITILO III 39
3. METODOLOGÍA 39
3.1. Método de la Investigación 39
3.2. Tipo de Investigación 40
3.3. Técnicas e Instrumentos de Investigación 41
3.4. Criterio de Inclusión y Criterio de Exclusión 41
3.5. Población y Muestra 42
CAPITULO IV 43
4. RESULTADOS Y DISCUSIÓN 43
4.1. Resultados 43
4.2. Encuestas 48
CAPÍTILO V 58
5. CONCLUSIONES Y RECOMENDACIONES 58
5.1. Conclusiones 58
5.2. Recomendaciones 59
Bibliografía 60
Lexigrafía 63
Infografía 63

TITULO

"ANÁLISIS JURÍDICO DE LA VENTA DE DATOS PERSONALES POR EMPRESAS FRENTE AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU REGULACIÓN VIGENTE"

CAPITULO I

1. PROBLEMA

Título

"ANÁLISIS JURÍDICO DE LA VENTA DE DATOS PERSONALES POR EMPRESAS FRENTE AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU REGULACIÓN VIGENTE"

1.1.Resumen

El presente trabajo de investigación titulado "Análisis Jurídico de la Venta de Datos Personales por Empresas Frente al Derecho a la Protección de Datos Personales y su Regulación Vigente" tiene como finalidad hacer un análisis en primera instancia de las indiscriminadas prácticas de comercialización de datos personales en nuestro país; los efectos que causan estos actos aun cuando en la actualidad se encuentra en vigencia la Ley Orgánica de Protección de Datos Personales.

Actualmente hay que considerar que en la actualidad el entorno digital es de uso diario, es parte de la vida cotidiana, se ha vuelto indispensable; este factor ha dado lugar a que varias empresas manejen datos personales de los ciudadanos ya sean financieras, de educación, de salud, etc.; razón por la que los datos personales son considerados un activo valioso para empresas; es así que, la protección de estos datos se ha convertido en un derecho fundamental, directamente vinculado a la privacidad y la seguridad de las personas e incluso de su patrimonio.

Uno de los ejes centrales de la presente investigación es la revisión de la normativa vigente, tanto a nivel local como internacional; ya que es importante determinar el nivel de protección legal que da el estado a sus ciudadanos en lo que respecta a su información personal, actualmente digitalizada casi en su totalidad. En el estado ecuatoriano la Ley

Orgánica de Protección de Datos Personales es la norma fundamental y es la que regula el tratamiento de datos personales, estableciendo obligaciones claras para las empresas, como la obtención del consentimiento informado y la adopción de medidas de seguridad para proteger la información personal; sin embargo, al compararse con normativas internacionales, como el Reglamento General de Protección de Datos en Europa o la Ley General de Protección de Datos en Brasil por ejemplo, se identifican ciertas deficiencias en la capacidad de supervisión y sanción por parte de las autoridades ecuatorianas, lo que limita la efectividad de la ley en la práctica.

Es importante investigar acerca de cómo varias empresas que operan siguen prácticas globales de recolección y comercialización de datos que no siempre se alinean con las expectativas de la ley; pues se observan casos en los que la venta de datos personales ocurre sin el consentimiento adecuado de los titulares, lo que genera preocupaciones sobre la violación de los derechos de privacidad. A su vez, los ciudadanos muestran una falta de conocimiento sobre sus derechos en esta materia, lo que aumenta la vulnerabilidad ante el uso indebido de su información personal.

Para la realización de este trabajo se recurrirá a un tipo de investigación exploratoria, descriptiva y analítica utilizando los métodos que aporten a su realización como el cuantitativo, cualitativo; también se aplicará la revisión documental; todo esto apoyado en herramientas de campo como la encuesta y la entrevista.

Palabras clave: Protección de Datos Personales, Derecho de Privacidad, Consentimiento Informado, Comercialización de Datos Personales, Legalidad.

Abstract

The present research work titled "Legal Analysis of the Sale of Personal Data by Companies in Relation to the Right to Personal Data Protection and its Current Regulation" aims to analyze, in the first instance, the indiscriminate practices of personal data commercialization in our country and the effects caused by these actions, even though the Organic Law on Personal Data Protection is currently in force.

In today's context, it is essential to consider that the digital environment is used daily and has become an indispensable part of everyday life. This factor has allowed various companies—whether in finance, education, health, and other sectors—to manage citizens' personal data. Consequently, personal data is considered a valuable asset for companies. Therefore, the protection of this data has become a fundamental right, directly linked to individuals' privacy and security, and even their assets.

One of the core focuses of this research is the review of the current legal framework, both at the local and international levels. It is crucial to determine the level of legal protection provided by the state to its citizens regarding their personal information, which is now almost entirely digitized. In Ecuador, the Organic Law on Personal Data Protection is the primary regulation governing the processing of personal data, establishing clear obligations for companies, such as obtaining informed consent and adopting security measures to protect personal information. However, when compared to international regulations, such as the General Data Protection Regulation (GDPR) in Europe or Brazil's General Data Protection Law (LGPD), certain deficiencies in the Ecuadorian authorities' capacity for supervision and sanctioning are identified, which limits the law's effectiveness in practice.

It is important to investigate how several companies operating in the market follow global data collection and commercialization practices that do not always align with the expectations set by the law. Cases have been observed where personal data is sold without the proper consent of the data subjects, raising concerns about violations of privacy rights. Additionally, citizens demonstrate a lack of awareness about their rights in this area, increasing their vulnerability to the misuse of their personal information.

This research will employ an exploratory, descriptive, and analytical approach, utilizing both quantitative and qualitative methods to achieve its objectives. A documentary review will be conducted, supported by field tools such as surveys and interviews.

Keywords: Personal Data Protection, Right to Privacy, Informed Consent, Personal Data Commercialization, Legality.

1.2.Introducción

En la era digital, los datos personales se han convertido en uno de los activos más valiosos para las empresas y las instituciones públicas; el procesamiento y la comercialización de esta información sin un control adecuado puede generar violaciones a la privacidad, abusos en su uso y afectar los derechos fundamentales de las personas. Por ello, es imperativo que los estados regulen y aseguren legalmente la protección de los datos personales, estableciendo un marco legal que garantice el control y la seguridad de la información que circula en entornos digitales.

La era digital ha transformado radicalmente la manera en que la información es generada, almacenada y utilizada; este fenómeno ha llevado a la digitalización masiva de datos, convirtiéndolos en un recurso clave para el desarrollo económico, social y cultural de las sociedades modernas.

La digitalización de los datos si bien ha ayudado a facilitar tramites tanto a nivel empresarial, para entidades gubernamentales, para facilidad del individuo mismo en el desarrollo de su vida cotidiana; no es menos ciertos que ha revolucionado diversos sectores, desde la educación hasta la salud y el comercio. En palabras de María Fernanda Gómez, "los datos personales y transaccionales son el nuevo petróleo de la economía digital, ya que permiten la creación de productos y servicios personalizados" (Gómez, 2022, p. 34). Esta afirmación refleja la creciente importancia económica de los datos, que han pasado de ser simples registros administrativos a activos estratégicos.

En América Latina, la digitalización ha sido particularmente relevante para mejorar la inclusión financiera y el acceso a servicios esenciales. Por ejemplo, la implementación de plataformas digitales en el sector financiero ha permitido que millones de personas

accedan a créditos y servicios bancarios, contribuyendo al desarrollo económico de la región (Pérez, 2023, p. 47).

A pesar de sus beneficios, la digitalización de los datos ha generado una gran problemática, especialmente en términos de privacidad y seguridad. La investigadora Adriana Vargas destaca que "la falta de regulaciones claras y la debilidad institucional en muchos países latinoamericanos permiten que los datos sean utilizados de manera indiscriminada" (Vargas, 2021, p. 27). Este problema se agrava por la creciente sofisticación de los ciberataques, que han expuesto la vulnerabilidad de las infraestructuras digitales en la región.

Es necesario además puntualizar que a pesar de que la digitalización ha avanzado rápidamente, millones de personas en América Latina siguen sin acceso a internet y a las tecnologías necesarias para aprovechar plenamente sus beneficios. Según un informe de la Comisión Económica para América Latina y el Caribe, "el 30% de los hogares en la región carece de conectividad de calidad, lo que limita su participación en la economía digital" (CEPAL, 2022, p. 15).

Ahora bien, la digitalización también ofrece oportunidades significativas; una de las más destacadas es la posibilidad de mejorar la gestión de servicios públicos. Por ejemplo, sistemas de salud digitalizados pueden optimizar la atención médica y facilitar el acceso a la información clínica de los pacientes, como se ha visto en proyectos implementados en Chile y Uruguay (López & García, 2023).

Además, la digitalización abre puertas a la innovación y al emprendimiento, varias plataformas originarias de América Latina, demuestran cómo la economía digital puede generar empleos y fomentar el crecimiento económico; lo cual ha sido más notorio a raíz de la pandemia mundial; en donde estas fueron indispensables para mover la economía en

los estados. Estas nuevas empresas han sabido capitalizar el valor de los datos para ofrecer soluciones únicas en el mercado (Martínez, 2022).

La protección de datos personales está vinculada directamente con el derecho a la privacidad, reconocido como un derecho fundamental en diversas constituciones y tratados internacionales; en América Latina, la Constitución de Ecuador (2008), la Ley Orgánica de Protección de Datos Personales (2021), y otros marcos normativos en países como Brasil con su Ley General de Protección de Datos (LGPD), subrayan la importancia de garantizar que los individuos tengan control sobre su información personal (Cordero, 2021).

Este derecho no solo implica proteger la privacidad del individuo, sino que también abarca el respeto por su identidad y autonomía. Según López y Rivera (2019), la protección de los datos personales es esencial en un mundo interconectado donde el acceso a la información es más amplio que nunca; la falta de regulación efectiva puede llevar a abusos y violaciones a la privacidad, como ha ocurrido en varios casos recientes de filtraciones de datos o ventas indebidas de información personal sin el consentimiento del titular.

El uso indebido de datos personales puede tener graves consecuencias, tanto para los individuos como para las empresas y gobiernos que los gestionan; uno de los problemas más preocupantes es la comercialización de datos personales sin consentimiento, lo cual expone a los titulares de los datos a riesgos como el fraude, la suplantación de identidad, o la discriminación en el acceso a servicios. Según Valenzuela (2020), las bases de datos personales son a menudo comercializadas entre empresas para fines de marketing o investigaciones, sin que los titulares estén conscientes del uso que se le está dando a su información.

Además, la falta de regulación puede generar desigualdades, donde quienes tienen acceso a grandes volúmenes de información personal tienen más poder de influencia sobre decisiones económicas, políticas o sociales; lo que es particularmente evidente en las empresas tecnológicas que manejan enormes volúmenes de datos. En este sentido, Lobato (2019) argumenta que la asimetría de poder entre los titulares de los datos y las entidades que los procesan solo puede corregirse mediante la implementación de marcos legales estrictos que regulen el uso de estos datos y protejan los derechos de los ciudadanos.

Los avances tecnológicos y el uso masivo de los datos personales exigen una regulación eficaz que imponga límites claros sobre cómo se puede recolectar, procesar, almacenar y transferir esta información; en este contexto, la creación de leyes como la Ley Orgánica de Protección de Datos Personales (LOPDP) en nuestro país es un paso importante hacia la protección de la privacidad. Esta normativa no solo establece derechos para los titulares de los datos, como el derecho al acceso, rectificación, oposición y cancelación, sino que también impone obligaciones a las empresas y entidades que manejan datos (López & Rivera, 2019).

Por ejemplo, nuestra legislación obliga a las empresas a obtener el consentimiento informado de los titulares antes de tratar sus datos y a implementar medidas de seguridad adecuadas para proteger la información. Esta regulación también contempla sanciones en caso de incumplimiento, lo que incentiva a las empresas a cumplir con los principios de transparencia y responsabilidad (Cordero, 2021).

Es importante además la concienciación de los ciudadanos sobre sus derechos en materia de protección de datos; aunque existen leyes que protegen estos derechos, muchas personas desconocen cómo ejercerlos o a qué instituciones recurrir en caso de violaciones. La educación y formación sobre la importancia de la privacidad y la protección de datos

personales es esencial para garantizar que las personas puedan defender sus derechos (Valenzuela, 2020).

La importancia de realizar una investigación sobre la venta de datos personales en el contexto del derecho a la protección de datos y la regulación vigente radica en la necesidad de garantizar que los derechos fundamentales de los ciudadanos sean respetados. Además, permite evaluar cómo las empresas ecuatorianas están implementando la normativa de protección de datos, identificar brechas y proponer mejoras que favorezcan la confianza, la seguridad y el respeto a la privacidad en un entorno digital; con el crecimiento de la economía digital y el aumento en el valor de los datos personales, este trabajo es vital para comprender los desafíos actuales y proponer soluciones que aseguren la protección legal adecuada.

1.3. Planteamiento del Problema

En la era digital, el uso y tratamiento de los datos personales se ha convertido en un activo invaluable para las empresas; sin embargo, la proliferación de la venta de estos datos plantea serias preocupaciones legales, especialmente cuando se contrapone al derecho fundamental a la protección de los datos personales. Si bien es cierto en nuestro país, la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) ha intentado establecer un marco regulador para proteger los derechos de los titulares de los datos, pero aún persisten prácticas empresariales que podrían estar violando esta normativa.

El problema central de esta investigación radica en cómo las empresas están comercializando los datos personales y si dicha práctica se alinea con las disposiciones vigentes en la legislación ecuatoriana. La venta de datos sin el consentimiento adecuado o con fines que no han sido claramente definidos plantea un conflicto directo con los

derechos de los ciudadanos a la privacidad y al control de su información personal; además, la falta de transparencia en el manejo de los datos y la dificultad de los titulares para ejercer sus derechos complican aún más la situación.

Este problema implica no solo un análisis jurídico del marco normativo, sino también una evaluación de las prácticas empresariales actuales en el tratamiento y comercialización de los datos personales, y cómo estas prácticas pueden impactar los derechos fundamentales de los ciudadanos en el entorno digital.

1.4.Formulación del Problema

¿Cuáles son los mecanismos propuestos en la normativa vigente en nuestro país para efectivizar el derecho a la protección de datos personales con la finalidad de evitar que indiscriminadamente las empresas los vendan?

1.5.Hipótesis

La falta de una adecuada implementación y supervisión de la Ley Orgánica de Protección de Datos Personales permite que las empresas comercialicen los datos personales de los ciudadanos, vulnerando el derecho a la privacidad y la protección de los datos personales de los titulares.

1.6.Variables

1.6.1. Variable Independiente

Implementación y supervisión de la Ley Orgánica de Protección de Datos Personales.

1.6.2. Variable Dependiente

La falta de una adecuada aplicación de la normativa permite que las empresas comercialicen los datos personales de los ciudadanos, vulnerando el derecho a la privacidad y la protección de los datos personales de los titulares.

1.7.Objetivos

1.7.1. Objetivo General

Analizar jurídicamente el derecho a la protección de datos personales, su regulación en la normativa estatal vigente frente a la venta de estos por parte de algunas empresas; sus efectos y consecuencias para los titulares de los datos.

1.7.2. Objetivos Específicos

Analizar la regulación normativa estatal con respecto a la protección de datos personales.

Identificar las practica empresariales en la venta de datos personales vulnerando los derechos de las personas.

Determinar los mecanismos para proteger los datos personales legalmente establecidos.

1.8.Justificación

La realización de un trabajo de investigación titulado "Análisis Jurídico de la Venta de Datos Personales por Empresas Frente al Derecho a la Protección de Datos Personales y su Regulación Vigente" es de suma importancia por varios motivos que afectan tanto a los derechos fundamentales de las personas como al cumplimiento de la normativa vigente en un entorno digital cada vez más dinámico y complejo; este análisis cobra relevancia en un contexto en el que el valor económico y estratégico de los datos personales está en

constante aumento, lo que genera una mayor necesidad de control y supervisión de su manejo por parte de las empresas.

El derecho a la privacidad y a la protección de datos personales es reconocido como un derecho fundamental en muchas jurisdicciones, incluyendo Ecuador, a través de la Ley Orgánica de Protección de Datos Personales promulgada en 2021; este derecho garantiza que los individuos mantengan control sobre la información que les identifica y que no sea utilizada sin su consentimiento.

La venta de datos personales sin los debidos controles y autorizaciones no solo constituye una vulneración de este derecho, sino que también genera riesgos de exposición a fraudes, discriminación o suplantación de identidad (Cordero, 2020). Esta investigación es clave para identificar en qué medida las empresas que manejan datos cumplen con la legislación y qué brechas persisten en su aplicación.

El auge de la economía digital ha hecho que los datos personales sean considerados el "nuevo petróleo" debido a su valor para actividades comerciales y estratégicas; lo que ha impulsado la creación de normativas como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Protección de Datos (LGPD) en Brasil, las cuales han servido de referencia para la legislación ecuatoriana. Sin embargo, la aplicación práctica de estas normativas aún presenta desafíos en países en vías de desarrollo, lo que hace que este estudio sea relevante para comprender el estado actual de la protección de datos en Ecuador y su alineación con los estándares internacionales.

El aumento de la comercialización de datos personales por parte de empresas ha generado preocupación a nivel global. Empresas de diversos sectores, desde tecnología hasta marketing, compran y venden grandes cantidades de datos para ofrecer productos personalizados o servicios más eficientes. Sin embargo, la falta de transparencia sobre

cómo se manejan y venden estos datos, y si los titulares han dado su consentimiento, plantea serios problemas legales y éticos (Lobato, 2018). Esta investigación es crucial para evaluar si las empresas en Ecuador están cumpliendo con las disposiciones de la LOPDP y para identificar prácticas que puedan estar afectando los derechos de los ciudadanos.

La confianza del consumidor es un pilar fundamental en las relaciones comerciales; las empresas que manejan datos personales sin cumplir con las normativas corren el riesgo de perder la confianza de sus clientes, lo que puede tener consecuencias negativas para su reputación y sus ingresos. Un análisis profundo de las prácticas actuales ayudará a comprender en qué medida las empresas están priorizando la protección de datos y cómo la responsabilidad corporativa puede jugar un papel esencial en la creación de políticas de manejo de datos más seguras y transparentes (Valdivieso, 2019).

Este estudio también tiene un valor significativo para la política pública, ya que puede proporcionar un diagnóstico claro sobre el estado de la regulación de protección de datos en Ecuador. Al identificar las brechas en la legislación o en su aplicación, se podrán hacer propuestas para mejorar las políticas públicas en esta área. Además, un análisis jurídico de este tipo es fundamental para fortalecer el marco regulatorio, asegurar su implementación efectiva y mejorar los mecanismos de control y sanción por parte de la autoridad de protección de datos (Pérez, 2020).

CAPITULO II

2. Marco Teórico

2.1.1. Concepto de Datos Personales y su Importancia Jurídica

Los datos personales se refieren a cualquier información relacionada con una persona física identificada o identificable; según la Ley Orgánica de Protección de Datos Personales, y en línea con el Reglamento General de Protección de Datos de la Unión Europea, los datos personales comprenden un amplio espectro de información que puede variar desde nombres, números de identificación, direcciones, hasta datos más sensibles como información genética, biométrica o financiera (GDPR, 2016). Según el Reglamento General de Protección de Datos, la identificación puede ser directa o indirecta.

El portal web de Grupo Ático 34; define a los datos personales y dice: “Los datos de carácter personal son toda información relativa a una persona física viva identificada o identificable. También son datos personales toda información que, recopilada y puesta en relación, pueda llevar a la identificación de una determinada persona.

Por lo tanto, los datos de carácter personal son toda aquella información relativa a personas físicas vivas que pueda usarse para identificarlas, tanto si se trata de información personal sobre su identidad como si es respecto a sus ocupaciones, hábitos o situación personal.” (https://protecciondatos-lopd.com/empresas/datos-personales/)

El artículo 4 de la Ley Orgánica de Protección de Datos del Ecuador define al “Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente. (LOPDP, 2021, p. 6) En conclusión se puede decir que un dato personal se refiere a cualquier información relacionada con una persona física que permita identificarla, directa o indirectamente; estas informaciones, que posibilitan la identificación de un individuo, se denominan datos de carácter personal, esto incluye cualquier dato que

permita reconocer directa o indirectamente a una persona, ya sea a través de elementos como el nombre, la fecha de nacimiento, el correo electrónico, el número de teléfono, la dirección física, características físicas, datos de ubicación u otros elementos que posibiliten vincular la información con un individuo específico, ya sea de forma directa o mediante un razonamiento razonablemente posible.

Es importante destacar que los datos personales no se limitan a registros escritos; también abarcan información visual o auditiva, como fotografías, grabaciones de audio o videos, siempre que permitan identificar a la persona a la que se refieren. Incluyen una variedad de información que permite identificar a una persona, ya sea directamente como: el nombre, la dirección o el número de identificación; o, indirectamente: a través de datos como la dirección IP o el historial de consumo, historial crediticio; a criterio de varios autores existen varios tipos de datos personales actualmente como por ejemplo: datos personales sensibles, datos personales biométricos, datos anonimizados.

Según De la Cueva (2020), los datos personales no solo constituyen información sensible, sino que también representan un punto de intersección entre tecnología, derechos humanos y regulación; esta concepción holística enfatiza que los datos personales no son un recurso aislado, sino un componente integral de la identidad de los individuos en un mundo globalizado.

La relevancia jurídica de los datos personales radica en su relación directa con derechos fundamentales; en nuestra legislación la Constitución de la República en su artículo 66, numeral 19, reconoce el derecho a la protección de datos personales, garantizando que el manejo de información se realice con respeto a la privacidad y la dignidad; este principio también está recogido en instrumentos internacionales como el

Reglamento General de Protección de Datos de la Unión Europea, que ha influido significativamente en las legislaciones latinoamericanas.

Desde una perspectiva jurídica, los datos personales requieren un tratamiento especial debido a su potencial para vulnerar derechos si son manejados de manera inadecuada; la exposición o uso indebido de datos puede dar lugar a discriminación, violación de la privacidad o incluso riesgos a la seguridad personal, especialmente en el contexto del ciberdelito y el espionaje digital.

Los datos personales son fundamentales en el mundo digital actual, ya que representan un recurso valioso para las empresas; sin embargo, su manejo y venta implican riesgos significativos relacionados con la privacidad y la autonomía de los individuos, lo que exige un marco normativo robusto que garantice la protección de estos derechos fundamentales.

2.1.2. Tipos de Datos Personales

La clasificación de los datos personales es una herramienta clave para entender cómo deben ser tratados, regulados y protegidos bajo marcos legales. Esta se la ha dado generalmente en la formalización de la norma que regula la protección de datos personales a nivel internacional y nacional; así se podría proponer la siguiente clasificación:

1. Datos Personales Básicos: Esta categoría abarca información común que permite identificar a una persona de manera directa. Entre los ejemplos más frecuentes se encuentran:

- Nombre completo.
- Fecha de nacimiento.
- Número de cédula.

- Dirección de correo electrónico.
- Números de teléfono.

Estos datos, aunque no sean especialmente sensibles, deben ser tratados bajo estrictas medidas de seguridad para prevenir accesos no autorizados o usos indebidos.

2. Datos Personales Sensibles: Los datos sensibles requieren un nivel de protección más elevado debido a que su uso indebido podría causar discriminación o daño significativo a la persona involucrada. De acuerdo con el Artículo 9 del Reglamento General de Protección de Datos de la Unión Europea; se consideran datos sensibles:

- Origen étnico o racial.
- Convicciones religiosas, filosóficas o políticas.
- Datos de salud, incluyendo el historial clínico y condiciones médicas.
- Información genética y biométrica.
- Vida sexual u orientación sexual.

3. Datos de Carácter Especial o Relacionados con Actividades Específicas: Esta categoría incluye información vinculada a condenas penales y delitos. El RGPD establece que su tratamiento debe ser realizado exclusivamente por autoridades competentes o bajo supervisión oficial, garantizando la protección de derechos fundamentales y evitando cualquier abuso.

4. Datos Anónimos y Pseudonimizados: Si bien no son considerados datos personales, los datos anónimos (aquellos que no pueden vincularse a una persona identificada o identificable) y los pseudonimizados (datos que han sido procesados para que no puedan atribuirse a una persona sin información adicional) también son relevantes

en el contexto de protección de datos. Estas técnicas reducen riesgos, pero siguen estando reguladas cuando es posible reidentificar a los individuos.

Conforme a la Ley Orgánica de Protección de Datos del estado ecuatoriano; los datos personales pueden ser:

Dato biométrico: La ley define al dato biométrico como una categoría de datos personales que identifica de manera única a una persona a través de características físicas, fisiológicas o conductas; ejemplos como imágenes faciales o datos dactiloscópicos son apropiados, pero podrían ampliarse a otros como patrones de voz, reconocimiento del iris o comportamientos digitales. Esta definición implica una relevancia especial en términos de seguridad, dado que los datos biométricos son irreversibles; es decir, una vez comprometidos, no pueden cambiarse como una contraseña.

Dato genético*:* La ley determina: "Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo."(LODPD, 2021). Este concepto destaca que los datos genéticos están relacionados con características heredadas o adquiridas que permiten identificar la fisiología o la salud de una persona, se subraya su naturaleza única. Es crucial que esta definición abarque el impacto en el ámbito de la privacidad médica y las posibles implicaciones discriminatorias, como el acceso al empleo o seguros, si se usan de manera indebida.

Dato personal: La definición básica de dato personal como cualquier información que identifique o haga identificable a una persona, ya sea de manera directa o indirecta; este enunciado sigue los estándares internacionales, como el Reglamento General de Protección de Datos (RGPD).

Datos personales crediticios: Se define este tipo de dato como aquellos que reflejan el comportamiento económico de las personas para analizar su capacidad financiera. Es una categoría sensible en términos de impacto socioeconómico, pues su tratamiento indebido podría generar consecuencias como la exclusión financiera o errores en calificaciones crediticias.

Datos relativos a: etnia, identidad de género, religión, orientación sexual, etc.: La ley Orgánica de Protección de Datos menciona datos que, por su naturaleza, son propensos a generar discriminación o afectar derechos fundamentales si son tratados de manera indebida. Además, se incluye información sobre personas apátridas o refugiadas, lo cual es relevante para el marco de derechos humanos.

Datos relativos a la salud: Estos datos se definen como aquellos que revelan información sobre el estado de salud física o mental de una persona, incluida la prestación de servicios sanitarios. La referencia a "prestación de servicios" añade una dimensión operativa en el ámbito médico; por lo que, es esencial asegurar altos niveles de protección para evitar usos indebidos, como discriminación laboral o seguros de salud restrictivos.

Datos sensibles: La definición de datos sensibles agrupa los datos mencionados anteriormente, destacando su potencial de discriminación y afectación a derechos fundamentales si se tratan de manera indebida. Es consistente con normativas internacionales, como el RGPD, que identifica este tipo de datos como de protección reforzada. La definición podría incluir ejemplos de medidas específicas para protegerlos.

Las definiciones son consistentes con estándares internacionales, pero podrían beneficiarse de una estructuración más clara, especialmente al diferenciar entre datos sensibles y otras categorías. Es importante considerar la implementación de principios de

protección, como la minimización de datos, consentimiento informado y medidas de seguridad específicas, para evitar tratamientos indebidos.

La clasificación de los datos personales es fundamental para garantizar su adecuado tratamiento y protección; ya que, cada tipo de dato requiere medidas específicas de seguridad que van desde el cifrado y la pseudonimización hasta la obtención de consentimientos claros y explícitos. Además, esta clasificación permite a las organizaciones cumplir con normativas legales, gestionar riesgos y proteger la confianza de los titulares de datos.

2.1.3. Evolución histórica de la legalización de los Datos Personales

La protección de datos personales ha evolucionado de manera significativa desde sus primeros antecedentes normativos hasta convertirse en un derecho fundamental reconocido a nivel internacional; esta transformación refleja la creciente importancia de salvaguardar la privacidad de las personas en un mundo digitalizado y globalizado.

El concepto de privacidad tiene sus bases filosóficas y jurídicas en el siglo XIX, cuando Samuel Warren y Louis Brandeis publicaron el artículo "The Right to Privacy" (1890), considerado el primer estudio formal sobre este derecho en los Estados Unidos; en él, los autores defendieron la necesidad de proteger la vida privada de las personas frente a los avances tecnológicos de la época, como la fotografía y los medios de comunicación impresos.

A nivel internacional, la privacidad se consagró como un derecho humano en el artículo 12 de la Declaración Universal de los Derechos Humanos (1948) y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966); estos instrumentos sentaron las bases para el desarrollo de normativas específicas de protección de datos personales.

La primera normativa específica sobre protección de datos personales surgió en Europa en respuesta a la creciente informatización de los datos en la segunda mitad del siglo XX. En 1970, Alemania aprobó la primera ley de protección de datos a nivel mundial: la Ley de Protección contra el Uso Abusivo de Datos Personales en Procesamiento Electrónico; este hito marcó el inicio de un movimiento regulatorio que se extendería por Europa y el resto del mundo.

En 1981, el Consejo de Europa adoptó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio 108), el primer instrumento internacional vinculante en esta materia; este convenio estableció principios fundamentales como la legalidad, proporcionalidad y seguridad en el tratamiento de datos personales.

Los avances en la Protección de Datos en las décadas de 1990 y 2000 se dieron con el auge de Internet y las tecnologías de la información en la década de 1990, la necesidad de una regulación más robusta se hizo evidente. La Unión Europea lideró estos esfuerzos con la aprobación de la Directiva 95/46/CE sobre la protección de datos personales, que estableció un marco común para los estados miembros y enfatizó la necesidad de garantizar un nivel adecuado de protección en las transferencias internacionales de datos.

A nivel global, también se destacaron iniciativas como las Directrices de la OCDE sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales (1980), que promovieron principios similares para armonizar las legislaciones nacionales.

En 2016, la Unión Europea adoptó el Reglamento General de Protección de Datos (RGPD), que entró en vigor en mayo de 2018; este reglamento representa un punto de inflexión en la historia de la protección de datos, al establecer un marco unificado, extraterritorial y basado en derechos fundamentales.

El Reglamento General de Protección de Datos introdujo principios clave como la transparencia, el derecho al olvido, la portabilidad de los datos y la obligatoriedad del consentimiento informado; además, impuso sanciones significativas por incumplimiento, lo que incentivó a empresas y gobiernos a fortalecer sus políticas de protección de datos.

En América Latina, la protección de datos ha avanzado de manera desigual; países como Brasil, con la Ley General de Protección de Datos (LGPD) de 2018, y México, con su Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), han adoptado legislaciones robustas inspiradas en el Reglamento General de Protección de Datos de la Unión Europea.

En Ecuador, la aprobación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021 representó un avance importante; esta ley establece principios como la responsabilidad proactiva, el consentimiento informado y la protección de los derechos de los titulares de datos. Además, crea la Autoridad Nacional de Protección de Datos Personales, encargada de supervisar el cumplimiento de la normativa.

A pesar de los avances, la protección de datos enfrenta numerosos retos en la actualidad con el avance tecnológico acelerado y continuo, como el uso de tecnologías emergentes inteligencia artificial, la proliferación de ciberataques y la necesidad de armonizar legislaciones a nivel global. En el futuro, será determinante fortalecer la cooperación internacional y garantizar que las normas de protección de datos evolucionen al ritmo de los desarrollos tecnológicos.

2.1.4. El Derecho a la Protección de Datos de Carácter Personal

El derecho a la protección de datos personales se ha convertido en un pilar fundamental dentro del marco de los derechos humanos en la actualidad a nivel mundial; este derecho garantiza la facultad de los individuos de controlar la información que les

concierne, regulando su recopilación, almacenamiento, uso y difusión por parte de terceros. Con el avance tecnológico y el auge de la economía digital, la protección de datos no solo es un derecho individual, sino también un elemento esencial para preservar la confianza en el entorno digital.

El derecho a la protección de datos personales se encuentra consagrado en diversos instrumentos internacionales, como el Convenio 108 del Consejo de Europa (1981), el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (2016/679) y, a nivel regional, en legislaciones nacionales como la Ley Orgánica de Protección de Datos Personales en Ecuador, promulgada en 2021; este derecho otorga a los titulares de los datos una serie de prerrogativas, como el acceso, rectificación, cancelación y oposición al tratamiento de su información personal.

Según el Reglamento General de Protección de Datos de la Unión Europea, los datos personales se definen como "toda información sobre una persona física identificada o identificable" (Art. 4.1). Esto incluye desde nombres y direcciones hasta información biométrica y digital, como direcciones IP o historiales de navegación.

En Ecuador, la Constitución de 2008 consagra el derecho a la protección de datos personales en su artículo 66, numeral 19 que textualmente, determina: "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." (Constitución de la República, 2008)

El análisis jurídico del texto constitucional se enmarca dentro del derecho fundamental a la protección de datos personales, el cual se reconoce como un derecho

autónomo y vinculado a la protección de la intimidad, la autodeterminación informativa y la privacidad. A continuación, se desglosa el contenido desde un enfoque jurídico, tomando como referencia la normativa ecuatoriana y principios generales del derecho:

Derecho a la protección de datos personales

La disposición constitucional establece claramente que el derecho a la protección de datos personales; que incluye el acceso y la decisión sobre la información, esto se relaciona con la autodeterminación informativa, que permite al titular de los datos decidir sobre el uso, acceso y destino de su información personal. Garantiza que los datos personales estén resguardados frente a usos indebidos o no autorizados.

Recolección, archivo, procesamiento, distribución y difusión

La disposición constitucional menciona las fases del tratamiento de datos personales, cada una de las cuales debe cumplir con ciertos principios y requisitos legales:

Recolección: La obtención de datos debe estar basada en:

El principio de licitud, es decir, que los datos solo se recolecten con autorización expresa del titular o conforme a lo dispuesto en la ley.

El principio de finalidad, que exige que los datos sean recolectados únicamente para propósitos específicos, explícitos y legítimos.

Archivo: El almacenamiento de datos implica garantizar:

Seguridad y confidencialidad, para evitar accesos no autorizados.

Limitación temporal, lo que significa que los datos no pueden ser almacenados más allá del tiempo necesario para cumplir con la finalidad.

Procesamiento: El tratamiento debe estar sujeto a:

Consentimiento informado, en el cual el titular conoce cómo serán procesados sus datos.

Minimización de datos, que exige que solo se procesen los datos estrictamente necesarios.

Distribución y difusión: Estos actos suponen un mayor riesgo para la privacidad, ya que implican compartir o hacer públicos los datos. Por ello, se requiere:

Consentimiento expreso y específico del titular.

Mandato legal, que debe ser claro y fundamentado en normativa específica.

Autorización del titular o mandato de la ley

La disposición constitucional subraya dos fuentes de legitimidad para el tratamiento de datos:

Autorización del titular: Esta autorización debe ser previa, libre, específica, informada y revocable. Se relaciona con el principio de consentimiento explícito, establecido en la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en Ecuador en mayo de 2021.

Mandato de la ley: Existen situaciones en las que el tratamiento de datos puede ser realizado sin el consentimiento del titular, siempre que esté respaldado por la ley, como en casos de interés público, cumplimiento de obligaciones legales, o por razones de seguridad nacional.

En el contexto ecuatoriano, el derecho a la protección de datos personales se reconoce como un derecho fundamental, garantizado en la Constitución y regulado

mediante la Ley Orgánica de Protección de Datos Personales (2021). Esta ley busca regular el tratamiento de datos personales y garantizar que las personas tengan control sobre la información que les pertenece.

2.1.5. Principios Rectores del Tratamiento de Datos Personales

Los principios rectores del tratamiento de los datos personales son normas fundamentales establecidas para regular las actividades relacionadas con la gestión de información personal; estos principios, recogidos en marcos legales internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y normativas nacionales como la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador, son esenciales para garantizar la legitimidad y transparencia en el tratamiento de datos.

Licitud, lealtad y transparencia

Este principio exige que el tratamiento de los datos sea realizado de manera legal, equitativa y transparente para los titulares. (ONU, 2021). Implica que las personas deben ser informadas claramente sobre el uso que se dará a sus datos y que este uso debe estar justificado en alguna de las bases legales establecidas.

Finalidad

Los datos personales deben ser recopilados con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines. (RGPDP, 2016). Este principio evita el uso arbitrario de los datos y garantiza que se respeten las expectativas de los titulares.

Los datos deben ser recolectados con fines legítimos y específicos, y no pueden ser utilizados de manera incompatible con esos fines (Ley Orgánica de Protección de Datos Personales, 2021).

Minimización de datos

Se debe limitar la recolección de datos al mínimo necesario para cumplir con la finalidad establecida, garantizando que solo se traten los datos estrictamente pertinentes (RGPD, 2016).Solo deben recopilarse los datos estrictamente necesarios para cumplir con los fines establecidos; este principio refuerza la idea de un tratamiento proporcional, reduciendo riesgos para la privacidad de las personas.

Exactitud

Los datos personales deben ser precisos y estar actualizados; los responsables del tratamiento deben adoptar medidas razonables para rectificar o eliminar información inexacta o incompleta.

Limitación del plazo de conservación

Los datos deben ser conservados solo durante el tiempo necesario para cumplir con los fines del tratamiento; una vez cumplida esta finalidad, deben ser eliminados o anonimizados, salvo que exista una obligación legal que justifique su conservación.

Integridad y confidencialidad

Este principio establece que los datos personales deben ser tratados de manera segura, implementando medidas técnicas y organizativas adecuadas para protegerlos contra accesos no autorizados, pérdida o destrucción.

Responsabilidad proactiva

Los responsables del tratamiento deben demostrar que cumplen con los principios rectores; este principio, también conocido como "accountability", implica la documentación y revisión constante de las prácticas de protección de datos.

Los principios rectores del tratamiento de los datos personales son pilares indispensables para garantizar un equilibrio entre el desarrollo tecnológico y la protección de los derechos individuales; la implementación rigurosa de estas normas es fundamental para enfrentar los desafíos actuales de la sociedad de la información y promover un uso ético y responsable de los datos. La aplicación de estos principios no solo protege los derechos fundamentales, sino que también fortalece la confianza de los ciudadanos en las instituciones y las empresas

Consentimiento: Los datos personales solo pueden ser procesados con el consentimiento libre, informado, específico y explícito del titular, salvo en excepciones legales.

Seguridad: Los responsables del tratamiento deben garantizar la seguridad de los datos para evitar su acceso no autorizado o su uso indebido.

2.1.6. La Autodeterminación Informativa

La autodeterminación informativa es un principio esencial en un mundo interconectado, donde la privacidad y el control sobre los datos personales son temas de creciente relevancia; este concepto, que se refiere al derecho de las personas a decidir sobre el uso de su información personal, adquiere una importancia trascendental ante el avance de las tecnologías digitales y el aumento exponencial del tratamiento de datos por parte de entidades públicas y privadas.

El derecho a la autodeterminación informativa tiene su base en la protección de los derechos fundamentales, como la privacidad y la dignidad humana. En el ámbito internacional, instrumentos como la Declaración Universal de los Derechos Humanos (1948) y el Pacto Internacional de Derechos Civiles y Políticos (1966) reconocen

implícitamente este derecho al garantizar la privacidad y la protección contra injerencias arbitrarias en la vida personal.

El desarrollo de la tecnología digital ha transformado la forma en que se recopilan, almacenan y utilizan los datos personales; las plataformas digitales, los algoritmos de inteligencia artificial y las bases de datos masivas han creado oportunidades sin precedentes, pero también riesgos significativos para la privacidad de los individuos.

La comercialización de datos personales, el uso de algoritmos discriminatorios y las violaciones de seguridad cibernética son ejemplos de cómo el uso indebido de la información personal puede afectar negativamente a las personas. En este contexto, la autodeterminación informativa no solo protege a los individuos de abusos, sino que también promueve la transparencia y la confianza en las instituciones.

Uno de los principales desafíos de la autodeterminación informativa radica en la falta de concienciación de los usuarios sobre sus derechos; a menudo, las personas aceptan términos y condiciones sin comprender plenamente las implicaciones del tratamiento de sus datos. Además, las empresas tecnológicas suelen emplear prácticas opacas que dificultan el ejercicio efectivo de este derecho.

Desde una perspectiva legal, es fundamental armonizar las normas nacionales con los estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que establece principios avanzados en materia de protección de datos y autodeterminación informativa. En Ecuador, la aplicación efectiva de la Ley Orgánica de Protección de Datos Personales requiere fortalecimiento institucional y educación ciudadana para garantizar su cumplimiento.

La autodeterminación informativa es fundamental para salvaguardar la privacidad y la dignidad en la era digital; su promoción y protección son esenciales no solo para

prevenir abusos, sino también para fomentar una cultura de respeto hacia los derechos de las personas en el ámbito digital. En este sentido, es imperativo que los estados, las empresas y la sociedad civil trabajen conjuntamente para garantizar que este derecho sea efectivamente reconocido y ejercido.

2.1.7. Normativa internacional y su influencia en la regulación ecuatoriana

La normativa ecuatoriana sobre protección de datos personales se inspira en estándares internacionales, especialmente el GDPR de la Unión Europea, considerado uno de los marcos legales más completos y estrictos en la protección de la privacidad. El GDPR ha servido de modelo para la LOPDP, especialmente en lo referente a la responsabilidad proactiva de las empresas, el derecho al olvido, la portabilidad de los datos y la transparencia en el tratamiento de la información.

A nivel latinoamericano, varios países han adoptado regulaciones similares, como la Ley de Protección de Datos de Brasil (LGPD), lo que ha generado una tendencia regional hacia el fortalecimiento de los derechos de los titulares de datos personales; en este sentido, Ecuador ha seguido esta tendencia global, aunque el desafío principal sigue siendo la implementación efectiva y el cumplimiento por parte de las empresas que manejan grandes volúmenes de datos.

2.1.8. La venta de los Datos personales

La venta de datos personales es una práctica cada vez más extendida en la era digital; las empresas recopilan, analizan y comercializan información sobre los usuarios, que va desde datos demográficos hasta patrones de comportamiento y preferencias de consumo. Aunque este intercambio de información genera beneficios económicos, también conlleva una serie de riesgos significativos para la privacidad y seguridad de las personas; los datos deben ser recolectados con fines legítimos y específicos, y no pueden ser

utilizados de manera incompatible con esos fines (Ley Orgánica de Protección de Datos Personales, 2021).

Desde un enfoque jurídico, la venta de datos personales se encuentra regulada por normativas que buscan garantizar los derechos fundamentales a la privacidad y a la protección de datos. En Ecuador, la Ley Orgánica de Protección de Datos Personales promulgada en 2021 establece en su artículo 25 dispone que el tratamiento de datos solo es lícito cuando existe consentimiento expreso, salvo en los casos excepcionales previstos por la ley; además, el artículo 29 regula específicamente la transferencia de datos a terceros, exigiendo que se garantice la seguridad de la información.

Antes de la aprobación de la Ley Orgánica de Protección de Datos exactamente en el año 2019; en el Diario "El Comercio" se desarrolla una noticia importe y que alarmo no solo al gobierno sino a todos los ciudadanos ecuatorianos; el titular era: "Los datos personales de millones de ecuatorianos están en manos de terceros y a la venta, dicen investigadores internacionales" (https://www.elcomercio.com/actualidad/negocios/venta-datos-ecuatorianos-investigadores-informatica.html).

El contenido de la nota informativa daba referencia a una investigación de dos expertos que descubrieron que millones de datos de los ciudadanos ecuatorianos fueron robados y que de manera alarmante se ofrecían suscripciones a la empresa "Novaestrat" en Miami para acceder a esos datos. Se enfatizó que se encontró información que incluía salarios, seguros de vida y una cantidad de datos privados que no deberían haber sido expuestos.

Los datos a los que se hace referencia en el medio de comunicación conforme los investigadores, contenía información personal sensible de 20 millones de ecuatorianos,

incluidos fallecidos y 6,7 millones de niños. Hubo una intervención legal estatal para bloquear el servidor internacional en aquel entonces.

El 26 de mayo del 2021 mediante Suplemento de Registro Oficial Nro. 459 entra en vigencia la Ley Orgánica de Protección de Datos en el estado ecuatoriano; y a pesar de que la norma determina literalmente la prohibición de datos personales, este mala practica se sigue utilizando e incluso un ciudadano común se puede dar cuenta de esto por cuanto recibe constantemente llamadas que el ofrecen servicios por su excelente manejo crediticio por ejemplo; existe

La venta de datos personales es un fenómeno complejo que requiere un abordaje multidimensional; la Ley Orgánica de Protección de Datos Personales, ofrece un marco jurídico sólido, pero su efectividad depende de la implementación de medidas técnicas y de una supervisión adecuada. Solo mediante un esfuerzo conjunto entre legisladores, técnicos y ciudadanos se podrá garantizar la protección de los derechos fundamentales en un mundo digitalizado.

2.1.9. Riesgos asociados a la venta de datos personales

La privacidad es uno de los derechos fundamentales más vulnerados por la venta de datos personales; cuando las empresas venden esta información sin el consentimiento informado de los usuarios, se transgrede el principio de autodeterminación informativa. En muchos casos, los términos y condiciones de los servicios digitales incluyen cláusulas ambiguas que permiten la comercialización de los datos, dejando a los usuarios en desventaja; además, la falta de transparencia en los procesos de recopilación y venta de información dificulta que las personas conozcan cómo y para qué se utilizan sus datos.

La venta de datos personales plantea varios riesgos que afectan tanto a los individuos como a las empresas; entre los riesgos más destacados están:

Violación de la privacidad: La venta de datos sin consentimiento explícito vulnera el derecho a la privacidad de los individuos, exponiéndolos a posibles abusos.

Discriminación: La venta de datos, especialmente información sensible, puede llevar a discriminación en ámbitos como la contratación laboral o el acceso a servicios.

Exposición a ciberdelitos: La comercialización de grandes bases de datos aumenta el riesgo de que esta información caiga en manos de actores malintencionados que la utilicen para cometer fraudes, suplantación de identidad o ataques de phishing.

La venta de datos personales también aumenta el riesgo de violaciones de seguridad; los datos pueden ser utilizados por ciberdelincuentes para cometer delitos como el robo de identidad, fraudes financieros y ataques de phishing. Según un informe de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), en América Latina y el Caribe, los incidentes de seguridad cibernética han aumentado exponencialmente en los últimos años, siendo los datos personales un objetivo principal (OEA & BID, 2021).

La comercialización de datos puede exacerbar desigualdades sociales; por ejemplo: las empresas podrían utilizar los datos para discriminar a ciertos grupos mediante estrategias de precios personalizados o acceso diferenciado a bienes y servicios. Además, la falta de control sobre los datos puede generar desconfianza en las plataformas digitales, afectando la participación ciudadana y el desarrollo económico.

En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en 2021, establece un marco para la gestión responsable de los datos personales; esta normativa promueve el consentimiento informado y refuerza los derechos de los titulares de los datos, como el acceso, la rectificación y la eliminación de la información. Sin embargo, su aplicación efectiva enfrenta retos como la falta de

concienciación ciudadana y la necesidad de fortalecer las capacidades de los órganos reguladores.

Más allá de las leyes, las empresas tienen una responsabilidad ética en el manejo de los datos personales; esto implica adoptar prácticas de privacidad por diseño, minimizar la recopilación de datos y garantizar la seguridad de la información. También es fundamental fomentar una cultura organizacional que priorice la transparencia y el respeto por los derechos de los usuarios.

La venta de datos personales representa un fenómeno complejo con implicaciones profundas en la privacidad, seguridad y equidad social; si bien las legislaciones como la Ley Orgánica de Protección de Datos Personales constituyen un paso importante hacia la protección de los derechos de los usuarios, es fundamental combinar estas iniciativas con esfuerzos éticos y tecnológicos para mitigar los riesgos asociados. Solo a través de una colaboración activa entre gobiernos, empresas y ciudadanos se podrá garantizar un entorno digital seguro y justo.

2.1.10. Sanciones y responsabilidades

La venta de datos personales sin autorización constituye una grave infracción a los derechos fundamentales protegidos por la Ley Orgánica de Protección de Datos Personales; las sanciones administrativas, civiles y penales previstas en la normativa tienen un doble propósito: disuadir a las organizaciones y particulares de incurrir en estas prácticas y garantizar la reparación del daño causado a las víctimas. En última instancia, el cumplimiento estricto de las disposiciones constantes en la ley es prioritario no solo para evitar sanciones, sino también para fomentar una cultura de respeto y protección de la privacidad en el Ecuador.

La Ley Orgánica de Protección de Datos Personales representa un hito fundamental en la garantía y protección del derecho a la privacidad y la autodeterminación informativa; en un contexto donde el manejo indiscriminado de datos personales se ha vuelto una práctica común en sectores tanto públicos como privados, esta normativa establece un marco legal para regular las acciones de quienes tratan información personal y para sancionar conductas que vulneren los derechos de las personas. Entre estas conductas, destaca la venta no autorizada de datos personales, un acto que acarrea importantes sanciones y responsabilidades.

De acuerdo con la norma, los datos personales solo pueden ser tratados si existe un consentimiento libre, específico, informado e inequívoco por parte del titular.; este principio constituye una barrera contra la comercialización de información personal sin la autorización expresa de las personas involucradas.

La ley también clasifica los datos en diferentes categorías, como datos personales sensibles, datos biométricos y datos de menores de edad, estableciendo mayores restricciones para el tratamiento de información considerada crítica; en consecuencia, la venta de datos personales sensibles sin autorización se considera una infracción particularmente grave.

La normativa estatal establece un régimen sancionador claro para quienes incumplan con las disposiciones de la ley; las sanciones administrativas son impuestas por la Autoridad de Protección de Datos y pueden clasificarse en leves, graves y muy graves, dependiendo de la naturaleza y alcance de la infracción.

En el caso de la venta no autorizada de datos personales, las sanciones aplicables suelen ser graves o muy graves, ya que esta práctica implica una vulneración directa de los derechos del titular de los datos. Las sanciones pueden incluir multas económicas que

varían entre el 0,1% y el 1% del volumen de negocios anual de la empresa responsable o montos fijos que oscilan entre los 10 y 100 salarios básicos unificados; además, en los casos más graves, la autoridad puede ordenar la suspensión de las actividades de la entidad infractora o la revocación de sus autorizaciones para operar.

La responsabilidad por la venta de datos personales no se limita a las sanciones administrativas; la LOPDP también contempla la posibilidad de que las personas afectadas interpongan acciones civiles por daños y perjuicios, en este sentido las víctimas de una filtración o venta no autorizada de sus datos tienen derecho a exigir una reparación integral, que puede incluir indemnizaciones económicas por el daño moral y material causado.

En el ámbito penal, el Código Orgánico Integral Penal (COIP) establece sanciones para quienes comercialicen información personal sin el consentimiento del titular; que influyen penas privativas de libertad, especialmente si la venta de datos ha ocasionado daños significativos o si se ha utilizado la información para cometer otros delitos, como estafas o suplantación de identidad.

La Ley Orgánica de Protección de Datos Personales impone a las organizaciones que tratan datos personales la obligación de implementar medidas de seguridad técnicas y organizativas adecuadas para prevenir accesos no autorizados y filtraciones de datos; esto incluye la adopción de políticas internas, la capacitación del personal y la realización de auditorías periódicas.

En caso de que se detecte la venta no autorizada de datos, no solo serán responsables los autores materiales del hecho, sino también los responsables y encargados del tratamiento que no hayan cumplido con su deber de diligencia. Por ello, las empresas

deben mantener un estricto control sobre el acceso y uso de la información personal que manejan.

CAPITILO III

3. METODOLOGÍA

Para la realización del presente trabajo de investigación, se utilizó una metodología basada en un enfoque exploratorio, descriptivo y analítico, utilizando métodos tanto cuantitativos como cualitativos. A continuación, se describe en detalle cada uno de los componentes metodológicos que guiarán el desarrollo de la investigación:

3.1.Método de la Investigación

Cuantitativo: Se utilizó para recolectar datos numéricos que proporcionen una visión general sobre las prácticas de venta de datos personales en nuestro país. Para ello, se aplicaron encuestas a ciudadanos y profesionales del derecho para medir el nivel de conocimiento sobre la protección de datos personales y las implicaciones legales de su comercialización.

Cualitativo: Mediante entrevistas en profundidad a expertos en derecho digital y protección de datos, se obtendrá una visión detallada y crítica sobre la aplicación de la normativa, las dificultades en su implementación y los desafíos actuales. Este método cualitativo permitió recoger opiniones especializadas y experiencias prácticas en el manejo de datos personales por parte de empresas.

Descriptivo: Se utilizó para detallar las características del marco normativo, las prácticas empresariales y los mecanismos de control que se encuentran vigentes. Se analizaron casos de ventas de datos personales y se describe cómo estas prácticas pueden impactar los derechos de los ciudadanos.

Analítico: El análisis se enfoca en evaluar la normativa vigente y su efectividad; a través del análisis jurídico de las leyes y de las prácticas empresariales, se podrá

determinar si la ley está siendo aplicada de manera eficiente y si los derechos de los titulares de los datos están suficientemente protegidos.

Exegético: Este método se centra en el análisis crítico y la interpretación de la normativa vigente, como la Ley Orgánica de Protección de Datos Personales y otras disposiciones relevantes. El método exegético permite interpretar cómo las disposiciones legales pueden ser aplicadas de manera práctica y cuáles son las lagunas que necesitan ser corregidas.

Revisión de la Normativa: La investigación incluye una revisión exhaustiva de la normativa ecuatoriana y comparativa, específicamente de la Ley Orgánica de Protección de Datos Personales, con especial énfasis en los artículos relacionados con la venta de datos personales y la protección de los derechos de los titulares. Además, se procedió a analizar otras normativas internacionales como el Reglamento General de Protección de Datos de la Unión Europea y la Ley General de Protección de Datos de Brasil para hacer comparaciones y sugerir mejoras a la legislación ecuatoriana.

3.2.Tipo de Investigación

Exploratoria: Este tipo de investigación es apropiado dado que el tema de la venta de datos personales en el contexto del marco legal ecuatoriano es un fenómeno relativamente nuevo. La investigación exploratoria permitió identificar patrones, problemas y áreas de oportunidad relacionadas con la comercialización de datos personales, así como los vacíos o deficiencias normativas en la Ley Orgánica de Protección de Datos Personales.

Descriptiva: Este enfoque permitió describir las prácticas actuales de las empresas en la venta y tratamiento de datos personales, así como los derechos de los titulares de los datos y las obligaciones de las empresas según la normativa vigente; se recolectó

información sobre cómo se comercializan los datos personales y el grado de conocimiento de los usuarios respecto a sus derechos.

Analítica: La investigación analítica permitió estudiar cómo la normativa actual regula la venta de datos personales, identificar las brechas legales, y evaluar si las empresas están cumpliendo con las obligaciones establecidas en la legislación. También se analizaron los posibles efectos de la falta de regulación adecuada sobre la privacidad de los ciudadanos.

3.3.Técnicas e Instrumentos de Investigación

Encuestas: Se aplicaron encuestas a un grupo de ciudadanos y profesionales del derecho para medir el nivel de conocimiento y percepción sobre el uso y la venta de sus datos personales, así como el grado de comprensión sobre sus derechos según la LOPDP. Estas encuestas proporcionaron datos cuantitativos para evaluar el impacto de la comercialización de los datos.

Entrevistas: Se realizaron entrevistas semiestructuradas con expertos en derecho digital, protección de datos y representantes de empresas que manejan grandes volúmenes de datos personales; estas permitieron obtener información cualitativa sobre la implementación de la normativa, los desafíos en la aplicación y las posibles mejoras en la protección de los datos personales.

3.4.Criterio de Inclusión y Criterio de Exclusión

El criterio de inclusión para aplicar las herramientas de campo de apoyo para el desarrollo de la investigación gira con respecto al conocimiento del tema, se tomó en cuenta a individuos que residan en el cantón Guaranda con conocimiento en el área de estudio; esto es: en lo que respecta a las entrevistas, se aplicaron a abogados especializados en derecho digital y protección de datos del cantón Guaranda en un número de 2; quienes

con su basto conocimiento en el tema aportaron al desarrollo de la investigación objetivamente.

En cuanto a las encuestas se tomó en cuenta a 50 ciudadanos para evaluar su nivel de conocimiento sobre la protección de sus datos personales con la característica de que conozcan acerca del manejo de los datos personales por varias empresas a nivel nacional para que emitan su criterio con respecto a la aplicabilidad de la protección de datos en nuestro país; todo esto, previo a la elaboración de un cuestionario técnicamente elaborado para que el resultado de lo consultado aporte positivamente a la investigación.

3.5.Población y Muestra

Entrevistas: 2 abogados expertos en Protección de Derechos Personales y Derecho Digital.

Encuestas: 50 ciudadanos del sector urbano del cantón Guaranda Provincia de Bolívar con la característica de que conozcan acerca del manejo de los datos personales por varias empresas a nivel nacional.

Localización geográfica del estudio: Casco Urbano, Cantón Guaranda, Provincia de Bolívar.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1.Resultados

Entrevista

Entrevistados: 2 abogados con conocimiento en Protección de Derechos Personales y Derecho Digital.

Ab. Esteban Meza (Entrevistado 1)

Ab. Sebastián Aragón Gaibor (Entrevistado 2)

De las entrevistas realizadas podemos concluir:

Pregunta 1

¿Qué se entiende por venta de datos personales y cómo se diferencia de otras formas de tratamiento de datos?

Entrevistado 1: Prácticamente es la comercialización de información personalísima de los ciudadanos. No hay diferencia el tratamiento de todos los datos personales como identificación, genética, salud, estados financieros deben ser resguardados y protegidos siempre porque el dueño de los mismos es el único que puede autorizar su utilización.

Entrevistado 2: Es cuando se hace mal uso de los datos personales de un individuo y se lo negocia, se lo comercializa en el mercado como si fuese cualquier bien mueble o inmueble. El tratamiento de datos debe ser siempre de uso delicado y manejados con consentimiento informado.

Pregunta 2

¿Qué principios fundamentales del derecho a la protección de datos personales se ven afectados por la venta de datos sin el consentimiento adecuado?

Entrevistado 1: Al venderse los datos personales se afectan todos los principios consagrados en las normas internacionales y nacionales, la protección misma, la intimidad, la transparencia, el buen uso, entre otros. Es una práctica ilegal.

Entrevistado 2: Es una ilegalidad vender los datos personales de los ciudadanos; es por esto que al cometer una ilegalidad se violenta todos los principios de la Constitución, los Tratados Internacionales y la ley; en cuanto a la Protección de Datos se violenta primordialmente el principio de transparencia, resguardo, seguridad, consentimiento informado y demás.

Pregunta 3

¿Existen prohibiciones legales en el Ecuador para la venta de datos personales, y cuáles son las sanciones establecidas para las empresas que incumplen con esta normativa?

Entrevistado 1: La ley Orgánica de Protección de Datos Personales contempla prohibiciones claras para la venta de los datos personales, recordemos que la norma está vigente desde el año 2021; incluso se contemplan infracciones de varios tipos para las empresas o personas que hagan mal uso de los datos personales confiados por los ciudadanos. Las sanciones son de tipo administrativo e inclusive puede convertirse en un delito conforme lo determina el Código Orgánico Integral Penal con el mal uso de os datos personales.

Entrevistado 2: La sanciones están estipuladas en la ley respectivamente; la Ley Orgánica de Protección de Datos contempla infracciones leves y graves que tienen que ver con el buen uso, buen manejo y protección de los datos personales estableciendo sanciones a su incumplimiento de carácter económico – multas; mientras que, el Código Orgánico Integral Penal con respecto a la protección de datos personales hace referencia a violación al derecho de intimidad que sanciona el mal uso de los datos personales con una pena privativa de la libertad que va desde 1 a 3 años.

Pregunta 4

¿Cuáles son las obligaciones de las empresas que recopilan y tratan datos personales bajo la Ley Orgánica de Protección de Datos Personales y cómo deben garantizar que no infringen los derechos de los titulares de los datos?

Entrevistado 1: El incumplimiento de las disposiciones legales contantes en la Constitución de la República y la Ley Orgánica de Protección de Datos Personales es una obligación para las empresas en nuestro país; además actualmente con la instauración de la Superintendencia de Protección de Datos las empresas tienen la obligación de contar con personal adecuado en el área informática y legal para implementar mecanismos seguros para la protección de los datos personales de los ciudadanos.

Entrevistado 2: Su obligación en primera instancia es que se convierten en custodios de los datos personales de los usuarios que confían en sus servicios y les proporcionan sus datos personales; ahora bien hay que mencionar que los datos personales son manejados tanto por instituciones públicas como privadas; es bajo este contexto que la Ley orgánica de Protección de Datos prácticamente contempla la creación de la Superintendencia de Protección de Datos; la misma que actualmente ya se encuentra en funcionamiento y que es la encargada de supervisar el cumplimiento de las disposiciones

legales en este aspecto. Además la normativa dispone que todas la instituciones tanto públicas como privadas tengan personal especializado en protección de datos para su custodia, manejo, buen uso y protección.

Pregunta 5

¿Cómo influye el consentimiento del titular de los datos en la legalidad de su venta y qué mecanismos deben emplear las empresas para obtener un consentimiento válido?

Entrevistado 1: El consentimiento del titular de los datos es fundamental para su utilización y manejo; es el único que puede autorizar formalmente su uso y manejo.

Entrevistado 2: Es la esencia legal del manejo y protección de datos el consentimiento informado del titular de los mismos; pues sin su autorización se imposible usar y manejar sus datos personales.

Pregunta 6

¿Qué brechas o vacíos legales existen en la regulación actual sobre la protección de datos personales en comparación con normativas internacionales?

Entrevistado 1: Protección ante la ciberdelincuencia, hay que asegurar más este aspecto en la ley.

Entrevistado 2: Prácticamente nuestra ley fue creada en armonía con normas internacionales, el problema es las nuevas modalidades de delitos que se producen y que tienen que ver con la conectividad, la tecnología que actualmente es muy peligroso; es en este aspecto que se tiene que reforzar la norma.

Pregunta 7

¿Cómo puede la venta de datos personales impactar negativamente en los derechos de privacidad y cómo afecta la confianza de los consumidores en las empresas que practican esta actividad?

Entrevistado 1: Afecta en todo sentido porque el uso de los datos personales de los ciudadanos de cualquier tipo es muy delicado y debe tener un tratamiento especial; así por ejemplo los datos de nombres, número de cédula, etc. pueden ser mal utilizados para cometer delitos y eso es muy peligroso; cuando hay mal manejo de setos lógicamente la desconfianza lesiona la actividades personales en todo sentido.

Entrevistado 2: El mal manejo de los datos personales lesiona gravemente el derecho a la intimidad y pone en riesgo la seguridad de la persona, recordemos que a través del uso de datos personales sacan cedulas falsa, visas, incluso se han hecho prestamos en entidades financieras de manera ilegal; por lo general son utilizados para el cometimiento de delitos; y cuando son manipulados en grandes volúmenes se expone a comunidades enteras a este tipo de inseguridad. La desconfianza creada por el mal uso afecta a quien mal manejo los datos y a las personas mismo.

4.2.Encuestas

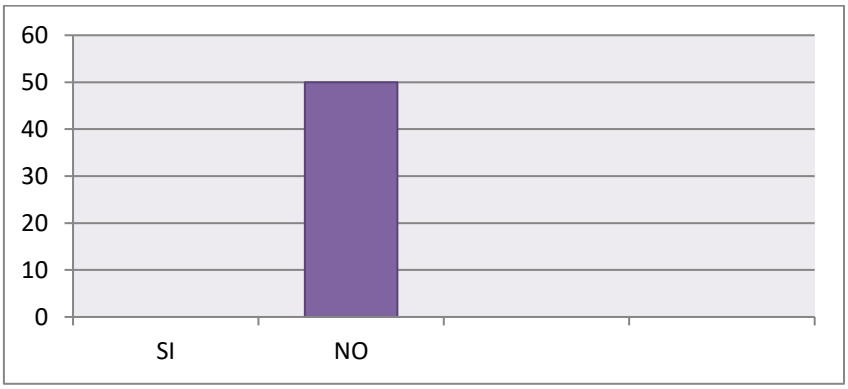
PREGUNTA 1

¿Conoce usted si las empresas que comercializan datos personales obtienen siempre el consentimiento informado de los titulares de los datos, según lo estipulado en la normativa ecuatoriana?

Tabla No. 1

SI	***NO***	***%***
o	***50***	***100%***

Gráfico No. 1



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: El cien por ciento de los ciudadanos encuestados desconoce acerca de la interrogante planteada con respecto a que las empresas que comercializan datos personales obtienen siempre el consentimiento informado de los titulares de los datos, según lo estipulado en la normativa ecuatoriana. Este resultado demuestra el desconocimiento de la población con respecto al manejo de sus datos personales por diversas empresas.

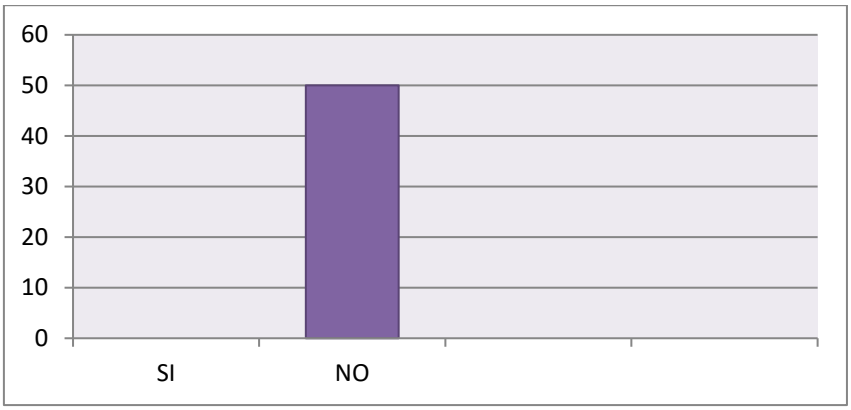
PREGUNTA 2

¿Cree usted que es legal en la actualidad la venta de datos personales sin restricciones?

Tabla No. 2

SI	*NO*	*%*
0	*50*	*100%*

Gráfico No. 2



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: Todos los ciudadanos encuestados consideran que no es legal en la actualidad la venta de datos personales sin restricciones. Este resultado tiene contradicción con el resultado de la pregunta uno; pues aquí se demuestra que tienen la percepción de que la venta de los datos personales es ilegal pero desconocen el tratamiento de los datos personales.

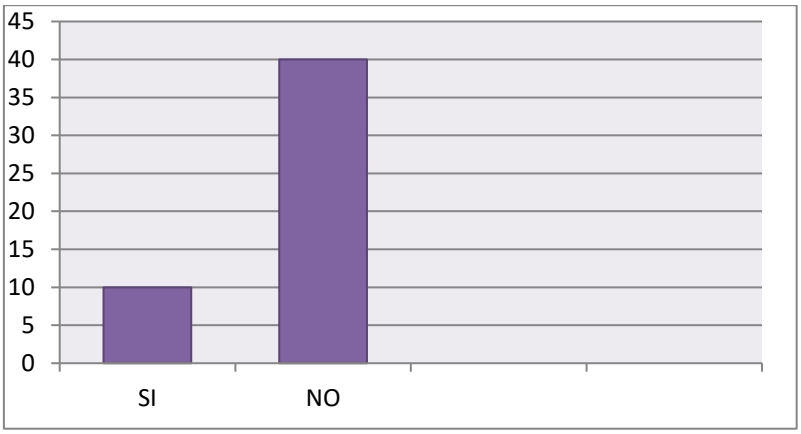
PREGUNTA 3

¿Tiene usted conocimiento del contenido de la Ley Orgánica de Protección de Datos Personales?

Tabla No. 3

SI	*NO*	*%*
10	***40***	***100%***

Gráfico No. 3



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: De los 50 ciudadanos encuestados la mayoría, específicamente 40 ciudadanos desconocen de la existencia de la Ley Orgánica de Protección de Datos Personales; mientras que 10 afirman conocerla. Es alto el índice de desconocimiento de la normativa, lo cual es alarmante por el uso constante de medios tecnológicos de las personas que incluyen su información personal.

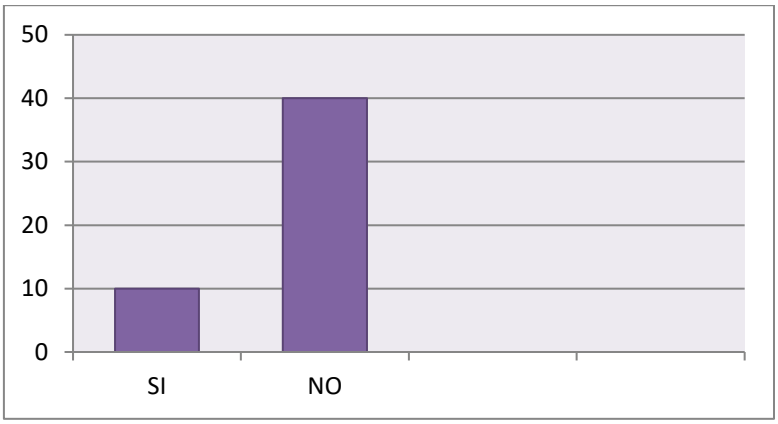
PREGUNTA 4

¿Conoce si los titulares de los datos personales tienen mecanismos claros y accesibles para revocar el consentimiento sobre el uso de su información personal?

Tabla No. 4

SI	***NO***	***%***
10	***40***	***100%***

Gráfico No. 4



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: cuarenta ciudadanos encuestados desconocen que los titulares de los datos personales tienen mecanismos claros y accesibles para revocar el consentimiento sobre el uso de su información personal; mientras que diez encuestados contestan afirmativamente interrogante planteado. El desconocimiento es general y llama mucho la atención por las consideraciones expuestas en los anteriores resultados.

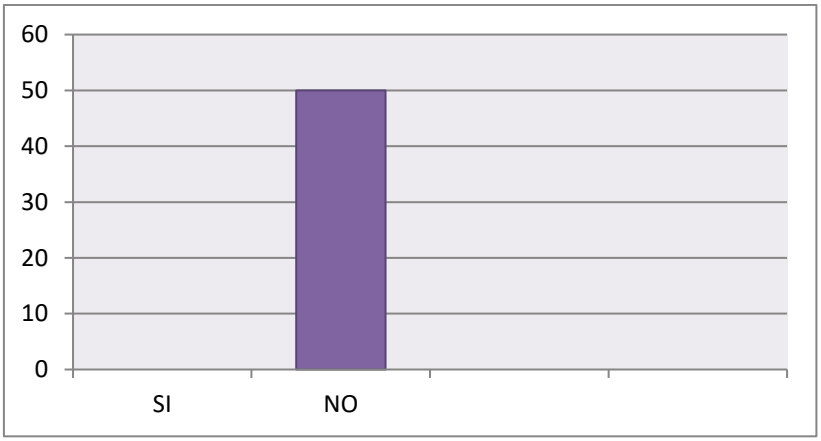
PREGUNTA 5

¿Conoce usted si la normativa vigente, La Ley Orgánica de Protección de Datos protege adecuadamente a sus ciudadanos frente a la transferencia de datos personales a otros países?

Tabla No. 5

SI	*NO*	*%*
0	***50***	***100%***

Gráfico No. 5



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: El cien por ciento de los ciudadanos contestaron de manera negativa, esto es que ellos creen que la Ley Orgánica de Protección de Datos Personales no protege adecuadamente a sus ciudadanos frente a la transferencia de datos personales a otros países. La ciudadanía a pesar de haber demostrado en respuestas anteriores desconocimiento de la normativa, en esta respuesta simplemente demuestran inseguridad a nivel general, siente que sus datos personales están desprotegidos.

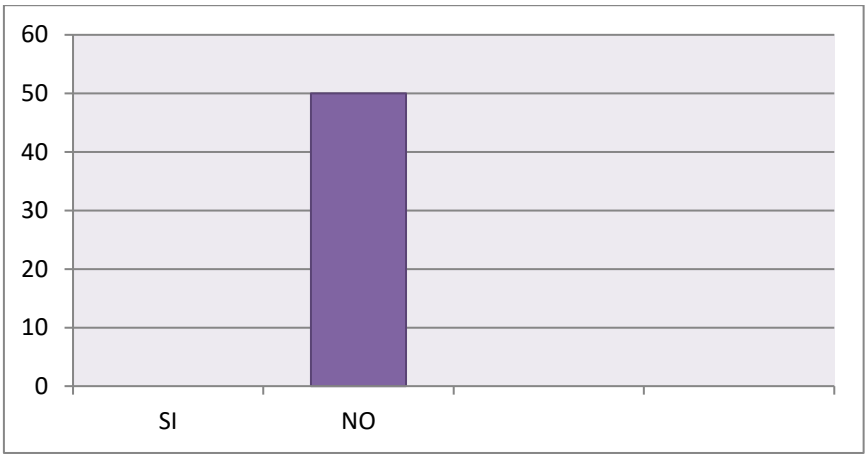
PREGUNTA 6

¿Sabe usted si la Ley Orgánica de Protección de Datos, protege los datos de las personales frente a su comercialización?

Tabla No. 6

SI	***NO***	***%***
0	***50***	***100%***

Gráfico No. 6



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: Todos los ciudadanos encuestados responden en esta interrogante negativamente; ósea, que desconocen si la Ley Orgánica de Protección de Datos protege los datos personales frente a su comercialización. El desconocimiento del contenido de la ley es evidente.

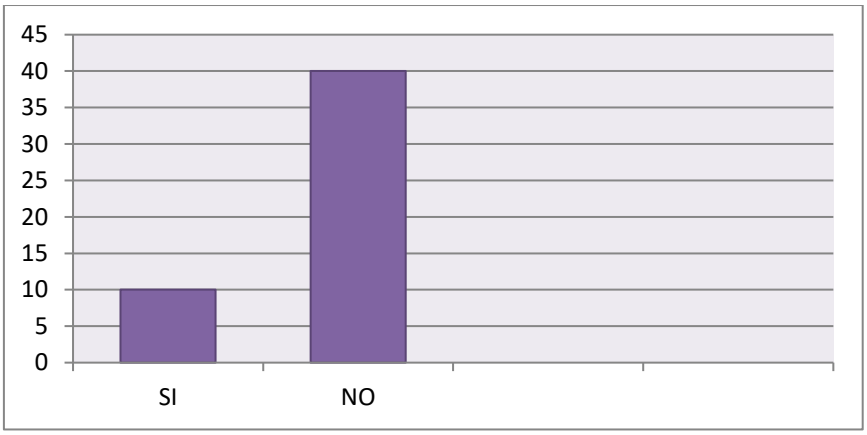
PREGUNTA 7

¿Conoce usted si la venta no autorizada de datos personales por empresas puede considerarse una violación directa al derecho a la Protección de Datos consagrado en la Constitución de la República del Ecuador?

Tabla No. 7

SI	***NO***	***%***
10	***40***	***100%***

Gráfico No. 7



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: En esta pregunta hay una variación en las respuestas, un tanto incomprensible por el resultado de las preguntas anteriores, exactamente la 5 y la 6; es así que, cuarenta ciudadanos responden negativamente y afirman creer que la venta no autorizada de datos personales por empresas no puede considerarse una violación directa al derecho a la protección de datos según la Constitución de la República del Ecuador. Mientras que diez ciudadanos contestan afirmativamente. Este resultado es confuso, prende una alarma de falta de socialización y concientización en la ciudadanía acerca del uso y manejo de los datos personales.

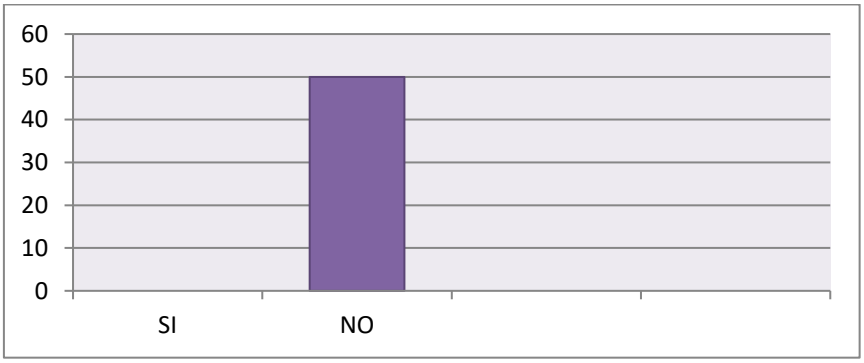
PREGUNTA 8

¿Conoce Usted que actualmente existe un organismo estatal que es la superintendencia de Protección de los Datos Personales que tiene la potestad de realizar controles para evitar el uso indebido o comercialización no autorizada de datos personales en el país?

Tabla No. 8

SI	*NO*	*%*
0	*50*	*100%*

Gráfico No. 8



Investigador: *Mayerlin Alejandra Guzmán Tocto.*

Población: *Ciudadanos del sector urbano, Cantón Guaranda, Provincia de Bolívar.*

ANÁLISIS: El cien por ciento de los ciudadanos encuestados dice no conocer de la existencia de la Superintendencia de Protección de Datos, entidad con la potestad de realizar controles para evitar el uso indebido o comercialización no autorizada de datos personales en el país. Desconocimiento total de la nueva entidad que ya funciona casi dos años en el país.

4.3.Discusión

La venta de datos personales por parte de empresas plantea un dilema complejo entre los intereses comerciales y la protección de los derechos fundamentales de las personas; esta investigación abordó la tensión existente entre estas dos dimensiones desde una perspectiva jurídica, teniendo en cuenta el marco normativo ecuatoriano e internacional vigente, así como los principios de privacidad y autonomía personal consagrados en diversos instrumentos legales.

En primer lugar, se identificó que la comercialización de datos personales es una práctica común entre empresas que operan en sectores como el comercio electrónico, la tecnología y el marketing digital; a pesar de la importancia económica de esta actividad, existe una preocupación creciente sobre las implicaciones éticas y jurídicas que esta conlleva, particularmente en el contexto de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador. La normativa establece principios como la legalidad, la transparencia y el consentimiento informado, los cuales no siempre se cumplen en las prácticas de venta de datos.

El análisis jurídico realizado evidencia que muchas empresas obtienen datos personales mediante cláusulas contractuales ambiguas o términos de servicio que no son completamente comprensibles para los usuarios; esta situación contraviene el principio de consentimiento informado, lo que genera una vulneración directa del derecho a la protección de datos personales garantizado por el artículo 66 de la Constitución de la República.

Además, se analizó las sanciones previstas en la Ley Orgánica de Protección de Datos Personales; la que no siempre son efectivas para disuadir las prácticas ilegales de venta de datos. En muchos casos, la falta de mecanismos robustos de supervisión y la

limitada capacidad de las autoridades competentes dificultan la aplicación de sanciones proporcionales y efectivas, este escenario fomenta una cultura de impunidad entre las empresas que priorizan sus beneficios económicos por sobre los derechos fundamentales de los ciudadanos.

Por otro lado, se identificó que la regulación ecuatoriana, si bien está alineada con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, presenta vacíos legales en cuanto a la responsabilidad de las empresas intermediarias y plataformas digitales. Esto permite que actores secundarios participen en el comercio de datos sin asumir responsabilidades claras.

En cuanto al aspecto internacional, se destaca que países con marcos regulatorios más estrictos han logrado una mayor protección de los datos personales de sus ciudadanos; por ejemplo, el GDPR impone sanciones severas y exige a las empresas un cumplimiento riguroso de los principios de protección de datos, estas experiencias ofrecen lecciones valiosas para el fortalecimiento del sistema ecuatoriano.

Por último, se enfatiza la necesidad de equilibrar el derecho a la protección de datos con los avances tecnológicos y las necesidades del mercado; es prioritario fomentar una cultura de respeto a los derechos digitales, que incluya la educación de los usuarios sobre la gestión de su información personal y la promoción de buenas prácticas empresariales.

El análisis realizado en el presente trabajo investigativo evidencia la urgencia de fortalecer la regulación vigente y de implementar mecanismos de cumplimiento más efectivos para garantizar la protección del derecho a la privacidad y a la autodeterminación informativa; sin estas medidas, el creciente fenómeno de la venta de datos personales continuará socavando los derechos fundamentales de los ciudadanos en un entorno digital cada vez más complejo y globalizado.

CAPÍTILO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El análisis de la normativa vigente evidencia que la protección de datos personales constituye un derecho fundamental, cuyo resguardo depende de un marco regulatorio actualizado. La existencia de leyes claras y mecanismos de supervisión efectiva es prioritaria para garantizar que el tratamiento de los datos se realice en cumplimiento con los principios de legalidad, transparencia, confidencialidad y consentimiento informado.

Se ha constatado que ciertas prácticas empresariales, como la venta o cesión de datos personales sin el consentimiento del titular, vulneran los derechos fundamentales a la privacidad y la autodeterminación informativa; estas acciones no solo revelan fallas en la ética corporativa, sino también la necesidad de una vigilancia más estricta por parte de las autoridades para prevenir y sancionar dichas conductas.

La existencia de mecanismos jurídicos, como la implementación de políticas de privacidad, las sanciones administrativas y penales, son esenciales para proteger los datos personales. Sin embargo, su efectividad depende de la sensibilización de los ciudadanos sobre sus derechos y del fortalecimiento institucional para garantizar el acceso a la justicia y la aplicación de medidas correctivas y punitivas frente a las violaciones de estos derechos.

5.2. Recomendaciones

Es fundamental que las autoridades legislativas revisen y actualicen periódicamente las leyes relacionadas con la protección de datos personales, incorporando estándares internacionales y nuevas tecnologías que garanticen un tratamiento de datos conforme a los principios de legalidad, transparencia, confidencialidad y consentimiento informado; además, se recomienda establecer mecanismos claros para la supervisión efectiva y sanciones más severas para quienes vulneren estas normativas.

Se recomienda reforzar la capacidad de los organismos de control para identificar, prevenir y sancionar prácticas empresariales que violen los derechos de privacidad y autodeterminación informativa; incluyendo la creación de auditorías regulares a las empresas que gestionan datos personales, así como la promoción de programas de certificación que garanticen el cumplimiento ético y legal en el manejo de información personal.

Es imprescindible desarrollar campañas educativas dirigidas a la ciudadanía para informarles sobre sus derechos en materia de protección de datos personales y los pasos necesarios para exigir su respeto. Simultáneamente, se deben optimizar los mecanismos de acceso a la justicia, como el habeas data, asegurando que las personas puedan denunciar violaciones de manera eficiente y recibir una respuesta ágil y efectiva por parte de las autoridades competentes.

Bibliografía

Autoridad de Protección de Datos de Brasil. (2018). Ley General de Protección de Datos (LGPD). Recuperado de https://www.lgpdbrasil.com.br

Brandeis, L., & Warren, S. (1890). El derecho a la privacidad. Harvard Law Review.

Castro, A. (2018). Protección de Datos Personales en la Era de las Redes Sociales. México D.F.: UNAM.

Comisión Económica para América Latina y el Caribe (CEPAL). (2022). Informe sobre conectividad y brecha digital en América Latina. Santiago de Chile: CEPAL.

Consejo de Europa. (1981). Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108). Recuperado de https://www.coe.int

Cordero, J. (2020). Protección de Datos Personales en el Ecuador: Análisis Comparativo con el GDPR. Editorial Jurídica.

Cordero, J. (2021). Protección de Datos Personales en Ecuador: Un análisis de la Ley Orgánica de Protección de Datos Personales. Quito: Editorial Jurídica.

De la Cueva, P. (2020). Protección de datos personales y derechos fundamentales en la era digital. Editorial Jurídica.

Garzón, I. (2021). Protección de Datos Personales y Derechos Humanos en América Latina. Quito: Universidad San Francisco de Quito.

Gómez, F. (2017). El Derecho a la Privacidad en la Legislación Española y Latinoamericana. Madrid: Editorial Dykinson.

Gómez, M. F. (2022). La economía digital y el valor de los datos en América Latina. Ciudad de México: Fondo de Cultura Económica.

Gutiérrez, E. (2016). El Derecho a la Protección de Datos Personales en el Marco Jurídico Internacional. Madrid: Ediciones Paraninfo.

Lobato, R. (2019). Desafíos del Derecho a la Privacidad en la Era Digital. Bogotá: Ediciones Legales.

López, J., & García, P. (2023). Innovación y salud digital en el Cono Sur. Montevideo: Editorial Sudamericana.

López, P., & Rivera, M. (2019). La Protección de Datos Personales en América Latina: Un Enfoque Comparado. Buenos Aires: Ediciones Jurídicas Latinoamericanas.

Luna, R., & Villegas, M. (2022). Regulación y protección de datos en América Latina: Retos y oportunidades. Revista Latinoamericana de Derecho Digital, 15(3), 45-62.

Martínez, L. (2019). La Protección de Datos en el Contexto del Big Data y la Inteligencia Artificial. Bogotá: Editorial Legis.

Martínez, R. (2022). "El impacto del emprendimiento digital en América Latina". Revista de Economía Digital, 18(2), 25-37.

Mendoza, C. (2019). Impacto de la Regulación Europea de Protección de Datos (GDPR) en Latinoamérica. Madrid: Tecnos.

Morales, S. (2020). Regulación y Protección de Datos en la Economía Digital. Lima: Pontificia Universidad Católica del Perú.

Muñoz, D. (2019). Nuevas Tendencias en la Protección de Datos Personales en el Mundo Digital. Caracas: Universidad Central de Venezuela.

Organización para la Cooperación y el Desarrollo Económico (OCDE). (1980). Directrices sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales.

Organización de Estados Americanos (OEA) & Banco Interamericano de Desarrollo (BID). (2021). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. https://www.oas.org/es/

Ortega, J. (2017). Protección de Datos y Privacidad en España: Análisis de la Ley Orgánica 15/1999. Barcelona: Editorial Aranzadi.

Paredes, J. (2021). El Rol de las Autoridades de Control en la Protección de Datos Personales. Quito: Universidad Andina Simón Bolívar.

Pérez, A. (2023). Inclusión financiera y tecnología en América Latina. Bogotá: Universidad de los Andes.

Pérez, C. (2020). Políticas Públicas y Protección de Datos Personales en Ecuador: Evaluación y Propuestas. Quito: Editorial Jurídica Andina.

Reyes, H. (2017). Marco Normativo para la Protección de Datos Personales en México. Ciudad de México: Porrúa.

Rodríguez, M. (2018). Protección de Datos en el Ámbito Empresarial: Marco Normativo y Desafíos. Buenos Aires: Universidad Austral.

Sánchez, A. (2018). Regulación de Datos Personales en España y América Latina: Retos y Oportunidades. Sevilla: Universidad de Sevilla.

Solove, D. J. (2020). Entendiendo la privacidad (2ª ed.). Harvard University Press.

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 (RGPD).

Valdivieso, P. (2020). La Protección de Datos Personales y la Responsabilidad de las Empresas. Guayaquil: Universidad Católica de Santiago de Guayaquil.

Valenzuela, A. (2020). Regulación de la Comercialización de Datos Personales en América Latina. Santiago: Universidad de Chile.

Vargas, A. (2021). "Privacidad y protección de datos en el contexto latinoamericano". Revista de Derecho y Tecnología, 9(3), 22-35.

Vázquez, R. (2020). La Evolución del Derecho a la Privacidad y la Protección de Datos. Buenos Aires: Abeledo Perrot.

Zuboff, S. (2019). La era del capitalismo de vigilancia. PublicAffairs.

Lexigrafía

Constitución de la República del Ecuador. (2008). Registro Oficial Suplemento 449 de 20 de octubre de 2008. Quito: Asamblea Constituyente.

Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459 de 26-may.-2021

Reglamento a la Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 435 de 13 de noviembre del 2023

Infografía

https://protecciondatos-lopd.com/empresas/datos-personales/

https://www.elcomercio.com/actualidad/negocios/venta-datos-ecuatorianos-investigadores-informatica.html