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 DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN"

Investigadora:

Melany Iveth Garcés Llanos

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 **Melany Iveth Garcés Llanos,** 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 DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN";** 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 Marianela Ruiz Abril

Tutora

DECLARACIÓN JURAMENTADA DE AUTENTICIDAD DE AUTORÍA

Yo; **MELANY IVETH GARCÉS LLANOS**, 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 DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN";** 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.

Atentamente,

MELANY IVETH GARCÉS LLANOS

Autora

DERECHOS DE AUTOR

Yo, Melany Iveth Garcés Llanos, portadora de la Cédula de Identidad No 0202292934 en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación: "ANÁLISIS DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN", 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 favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo 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 autor declara 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.

MELANY IVETH GARCÉS LLANOS
FIRMA

DEDICATORIA

Con mucho amor, cariño y respeto quiero dedicar esta tesis principalmente a mis padres Ing. Angel Garces y Lic. Ana Llanos que han sido mi principal apoyo durante este largo camino.

Mi hermana Lic. Janelly Garces que ha sido parte fundamental en esta fase de mi vida.

A mis abuelitos Mario y Juanita quienes me han brindado su apoyo siempre y a quienes considero mis segundos padres, ya que con su complicidad me han ayudado incondicionalmente.

Terminar esta etapa de mi vida ha sido el resultado de mucho esfuerzo y dedicación propia, por eso también esta tesis me la dedico a mí, porque es una muestra de lo fuerte que he sido durante todo este tiempo y de lo mucho que puedo lograr junto a mis seres queridos.

Melany

AGRADECIMIENTO

Quiero agradecer principalmente a Dios por permitirme cumplir este sueño que he tenido durante años.

Agradezco también a mis padres Anita y Ángel por no haberme dejado sola y ser mi pilar fundamental en todo este proceso, ya que con su esfuerzo de cada día me permitían seguir adelante.

A mi hermana Janelly por haberme ayudado durante toda mi etapa Universitaria, por ser mi cómplice y apoyo a lo largo de mi vida.

Mis abuelitos Juanita y Mario, que con su amor incondicional y su apoyo he logrado seguir adelante cumpliendo todas mis metas.

A mi abuelita Marianita y demás familiares que han confiado en mí y me han ayudado a superar esta etapa de mi vida.

Agradezco a mis profesores que con su conocimiento y dedicación he logrado culminar mi carrera, también a mis amigos que desde el inicio hasta el final han sido parte de este proceso.

Melany Iveth Garcés Llanos

Tabla de contenido

TITULO

"ANÁLISIS DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN"

CAPITULO I

1. PROBLEMA

Título

"ANÁLISIS DE LOS MECANISMOS JURÍDICOS ESTABLECIDOS EN LA LEGISLACIÓN ECUATORIANA PARA PROTEGER LOS DATOS PERSONALES DE LAS PERSONAS EN LA ERA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN"

1.1.Resumen

El presente trabajo de investigación titulado "Análisis de los mecanismos jurídicos establecidos en la legislación ecuatoriana para proteger los datos personales de las personas en la era de las tecnologías de la información"; como su título lo señala tiene como finalidad de determinar la existencia de mecanismos jurídicos que consten en la legislación actual para salvaguardar los datos personales de los ciudadanos; situación que en la época en la que vivimos se ha hecho emergente por el avance agigantado de las Tecnologías de la Información y la Comunicación, con ello van apareciendo problemas legales por darse situaciones de abuso de los datos personales de los ciudadanos, irrespeto a su derecho constitucional a la intimidad y a la privacidad; también se ve afectado su derecho a la autodeterminación informativa, violentando incluso el derecho al consentimiento informado en lo que ha tratamiento de los datos personales se refiere.

La protección de los datos personales ha adquirido mayor relevancia en los últimos tiempos, más aún con el uso ineludible y constante del almacenamiento digital de la información tanto en los niveles gubernamentales públicos como en el ámbito privado. Es bien conocido por todos que, desde la década de los años 90, con la expansión de Internet y las circunstancias ya expuestas en anteriores líneas; el desarrollo tecnológico permitió un

acceso sin precedentes a grandes volúmenes de datos, lo que generó preocupación por la vulnerabilidad de la información personal.

Con la llegada de las redes sociales, el comercio electrónico y la digitalización de los servicios públicos, se hizo evidente la necesidad de regular el uso y protección de los datos personales, lo que impulsó una actualización y creación de normativas específicas; en el caso específico del estado ecuatoriano mediante Registro Oficial Suplemento 459 de 26 de mayo del 2021 se promulgo la Ley Orgánica de Protección de Datos Personales; normativa que tiene como objetivo garantizar el derecho a la protección de los datos personales, lo que incluye el acceso y control sobre dicha información, así como su adecuada protección; para lo cual se establece principios, derechos, obligaciones y mecanismos de tutela relacionados con el manejo de los datos personales.

Analizar los mecanismos de protección de datos personales es indispensable por cuanto el uso masivo de tecnologías expone a los individuos a riesgos de privacidad; por este motivo es necesario que legalmente se asegure que la información personal sea tratada de manera lícita y transparente, evitando su uso indebido o la vulneración de los derechos fundamentales; más aún en la actualidad en donde las empresas y entidades públicas manejan grandes volúmenes de datos, situación ante la cual el estado legalmente debe garantizar la seguridad, confidencialidad y control de los titulares sobre su información.

La investigación es de tipo descriptiva y explicativa, utilizando los métodos analítico, inductivo y deductivo; con enfoque descriptivo se emplea para identificar y detallar los mecanismos jurídicos existentes. En este trabajo se analiza cómo estas normas han sido aplicadas en la práctica para garantizar la seguridad de los datos personales, considerando también la adhesión del estado ecuatoriano a tratados internacionales.

Palabras clave: Protección de Datos Personales, Derecho a la Intimidad, Derecho a la Privacidad, Consentimiento Informado, Principio de Legalidad.

Abstract

The present research work titled "Analysis of the Legal Mechanisms Established in Ecuadorian Legislation to Protect Personal Data in the Era of Information Technologies" aims, as its title indicates, to determine the existence of legal mechanisms within the current legislation to safeguard citizens' personal data. This issue has become increasingly urgent in the era we live in, due to the rapid advancements in Information and Communication Technologies. These advancements have brought about legal challenges, including the abuse of citizens' personal data, violations of their constitutional rights to privacy and intimacy, and the undermining of their right to informational self-determination. Furthermore, the right to informed consent concerning personal data processing is often violated.

The protection of personal data has gained greater relevance in recent years, especially given the unavoidable and constant use of digital information storage, both at public governmental levels and in the private sector. It is widely recognized that since the 1990s, with the expansion of the Internet and the circumstances outlined above, technological developments enabled unprecedented access to large volumes of data, raising concerns about the vulnerability of personal information.

With the advent of social networks, e-commerce, and the digitization of public services, the need to regulate the use and protection of personal data became evident. This led to the update and creation of specific regulations. In Ecuador, the Organic Law on Personal Data Protection was promulgated through Supplement No. 459 of the Official Register on May 26, 2021. This legislation aims to guarantee the right to personal data protection, which includes access to and control over such information, as well as its

adequate protection. To achieve this, the law establishes principles, rights, obligations, and protection mechanisms related to the handling of personal data.

Analyzing mechanisms for personal data protection is essential, given that the massive use of technology exposes individuals to privacy risks. For this reason, it is necessary to legally ensure that personal information is handled lawfully and transparently, preventing its misuse or the violation of fundamental rights. This is particularly relevant today, as companies and public entities manage large volumes of data. In this context, the state must legally guarantee the security, confidentiality, and control of individuals over their information.

This research is descriptive and explanatory, utilizing analytical, inductive, and deductive methods. A descriptive approach is employed to identify and detail the existing legal mechanisms. This study examines how these regulations have been applied in practice to ensure the security of personal data, also considering Ecuador's adherence to international treaties.

Keywords: Personal Data Protection, Right to Privacy, Right to Intimacy, Informed Consent, Principle of Legality.

1.2.Introducción

En la última década, el avance de las tecnologías de la información ha transformado radicalmente el panorama global, impactando diversos aspectos de la vida cotidiana, desde la economía hasta la interacción social; las innovaciones tecnológicas, como el uso de la inteligencia artificial, la computación en la nube, el big data y el internet, han permitido un acceso sin precedentes a la información y han generado nuevos modelos de negocios, mejorando la eficiencia y la productividad en casi todos los sectores (Castells, 2020). Sin embargo, estos avances también han traído consigo una seria problemática, particularmente en lo que respecta a la protección de los datos personales, ya que la digitalización masiva ha incrementado la vulnerabilidad de la información privada frente a diversos peligros, como la venta indiscriminada de bases de datos, el cibercrimen y la vigilancia masiva.

La proliferación de tecnologías disruptivas ha acelerado el proceso de digitalización a nivel global; el acceso a internet y el uso de dispositivos conectados a la red han aumentado exponencialmente, con más de 5.000 millones de usuarios de internet en todo el mundo para el año 2022, representando el 64% de la población global (Statista, 2022). Esta interconexión ha generado un vasto volumen de datos que se recopilan y procesan diariamente, lo que ha permitido la creación de perfiles detallados de las personas, empleados con fines comerciales y sociales. La integración de la inteligencia artificial en sectores como el comercio, la salud y la educación ha mejorado la toma de decisiones mediante el análisis predictivo y el procesamiento automatizado de grandes conjuntos de datos (González, 2019).

En América Latina, la adopción de estas tecnologías ha seguido una tendencia creciente.; así, países como Brasil, México y Argentina han experimentado un aumento significativo en el uso de la tecnología en sectores clave, como el financiero y el gubernamental, pero a pesar de este progreso, la región enfrenta importantes retos

tecnológicos y legales en términos de infraestructura digital y seguridad cibernética, lo que exacerba los riesgos asociados con la protección de datos personales (Maldonado, 2021).

Con el auge de las tecnologías de la información, ha surgido una creciente preocupación por los peligros relacionados con la protección de los datos personales; el aumento de ciberataques, como el robo de identidad y las violaciones de datos masivas, representa una amenaza constante para los usuarios. Según estudios recientes, América Latina experimentó un aumento del 24% en los ciberataques en 2021, lo que subraya la vulnerabilidad de la región ante estas amenazas (ESET, 2021).

Además, es necesario puntualizar que el creciente uso de tecnologías como el big data y la inteligencia artificial ha dado lugar a preocupaciones sobre la invasión de la privacidad; el procesamiento masivo de datos personales sin el consentimiento adecuado de los titulares puede derivar en la explotación comercial de dicha información, afectando los derechos fundamentales de los ciudadanos (Mendoza, 2020). En este sentido, la protección de los datos personales no solo es un tema de seguridad, sino también de ética, ya que la manipulación indebida de los datos puede tener graves consecuencias en la autonomía y libertad individual.

A nivel global, la preocupación por la protección de los datos personales comenzó a emerger en la década de 1970, cuando las primeras bases de datos electrónicas empezaron a ser utilizadas por gobiernos y empresas. Alemania fue uno de los primeros países en adoptar una ley sobre protección de datos en 1970, seguido de la Directiva Europea de Protección de Datos en 1995, que marcó un hito en la regulación de la privacidad de la información en Europa (Méndez, 2020). En América Latina, el desarrollo de leyes de protección de datos fue más lento, pero tomó impulso a partir de los años 2000 debido a la expansión del uso de Internet y el comercio electrónico.

La protección de los datos personales se ha convertido en una prioridad global, especialmente ante los riesgos que plantea el avance de las tecnologías de la información. La legislación sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley Orgánica de Protección de Datos Personales en Ecuador, han establecido marcos regulatorios robustos para garantizar que las entidades que procesan datos cumplan con principios básicos de transparencia, seguridad y confidencialidad (Romero, 2021).

La protección de los datos personales es esencial no solo para salvaguardar la privacidad de los individuos, sino también para mantener la confianza en las plataformas digitales. En este sentido, es fundamental que los gobiernos y las empresas adopten medidas proactivas para garantizar la seguridad de los datos, implementando políticas de privacidad claras y utilizando tecnologías avanzadas de cifrado y control de acceso. La educación de los usuarios también es clave, ya que la falta de conocimiento sobre los peligros asociados con el uso indiscriminado de la tecnología puede aumentar la exposición a riesgos (Gómez, 2019).

En el estado ecuatoriano, el reconocimiento del derecho a la privacidad y la protección de los datos personales tiene sus raíces en la Constitución de 2008, que en su artículo 66 reconoce el derecho de las personas a la protección de su información personal. Este fue el primer paso significativo hacia el establecimiento de un marco legal robusto, que luego se consolidaría con la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021; se podría afirmar que los mecanismos jurídicos establecidos para proteger los datos personales van implementándose y avanzando conforme a las nuevas realidades sociales.

La importancia de investigar acerca de la protección de los datos personales radica en varios factores clave que afectan tanto a los individuos como a la sociedad en general, especialmente en el contexto de la creciente digitalización y el uso masivo de las Tecnologías de la Información y la Comunicación.

La protección de los datos personales está intrínsecamente vinculada con el derecho a la privacidad, un derecho fundamental reconocido por la Constitución; por lo que, investigar sobre este tema permite garantizar que los ciudadanos puedan ejercer este derecho en un entorno digital cada vez más complejo y donde la información personal se convierte en un activo valioso para terceros; esta investigación contribuye a que se comprenda mejor cómo se pueden vulnerar estos derechos y qué mecanismos son necesarios para su protección efectiva.

1.3.Planteamiento del Problema

En la era de las tecnologías de la información, el avance exponencial de la digitalización y el uso masivo de datos personales plantea desafíos significativos en la protección del derecho a la vida privada de las personas. Si bien la protección legal de datos personales se presenta como un mecanismo fundamental para salvaguardar la intimidad en el entorno digital, surgen interrogantes sobre la efectividad y la suficiencia de las regulaciones existentes. La constante recopilación, almacenamiento y procesamiento de información personal por parte de entidades públicas y privadas, así como el desarrollo de tecnologías de análisis de datos, abre debates sobre la capacidad de las leyes actuales para proteger verdaderamente la esfera privada de los individuos. Esta situación plantea una problemática crucial ¿Son las regulaciones vigentes sobre protección de datos suficientes y eficaces para garantizar el derecho a la vida privada de las personas en un contexto digitalizado? En este sentido, se hace necesario un análisis profundo y crítico de las normativas existentes, su aplicabilidad en el contexto tecnológico actual y la pertinencia de

posibles ajustes legales para salvaguardar de manera efectiva el derecho a la vida privada en la era de las tecnologías de la información.

1.4. Formulación del Problema

¿En qué medida las regulaciones actuales sobre la protección legal de datos personales son eficaces y suficientes como mecanismo jurídico para preservar el derecho a la vida privada de las personas en el contexto de la creciente influencia de las tecnologías de la información?

1.5.Hipótesis

Los mecanismos jurídicos establecidos en la legislación ecuatoriana, específicamente en la Ley Orgánica de Protección de Datos Personales, es suficiente para garantizar la adecuada protección de los datos personales frente a las amenazas derivadas del uso de las tecnologías de la información.

1.6.Variables

1.6.1. Variable Independiente

Los mecanismos jurídicos establecidos en la Ley Orgánica de Protección de Datos Personales para la protección de datos personales.

1.6.2. Variable Dependiente

Son Suficientes para garantizar la adecuada protección de los datos personales frente a las amenazas derivadas del uso de las tecnologías de la información.

1.7.Objetivos

1.7.1. Objetivo General

Evaluar la efectividad y pertinencia de las regulaciones legales existentes en materia de protección de datos personales como mecanismo jurídico para resguardar el derecho a la vida privada de las personas en el contexto de la expansión de las tecnologías de la información.

1.7.2. Objetivos Específicos

Analizar el marco legal existente en el estado ecuatoriano relacionados con la protección de datos personales en el entorno digital.

Identificar los riesgos asociados al uso, almacenamiento y tratamiento de datos personales en la era de las tecnologías de la información.

Determinar la efectividad y alcance de las regulaciones actuales en la preservación de la privacidad y el control de los individuos sobre sus datos personales.

1.8.Justificación

La protección de los datos personales ha adquirido una relevancia central en la era de las tecnologías de la información, donde la digitalización y el uso masivo de redes interconectadas exponen a las personas a vulneraciones de su privacidad. En nuestro país, la legislación en esta materia ha evolucionado para responder a las nuevas demandas de un entorno digital, pero su implementación y efectividad en la protección de los derechos fundamentales requieren un análisis profundo. Esta investigación se justifica para determinar la pertinencia del marco legal vigente frente a los desafíos que presenta el avance tecnológico.

El derecho a la privacidad y la protección de los datos personales son derechos fundamentales reconocidos tanto en la Constitución como en instrumentos internacionales esta proclamada y dispuesta; no obstante, a pesar de la existencia de un marco normativo que busca proteger estos derechos, los avances tecnológicos han generado nuevas amenazas y riesgos que deben ser puestos en el tapete de la discusión para exponer la problemática actual.

Uno de los principales retos de nuestra legislación tiene que ver con su adaptación a los estándares internacionales en protección de datos, en un contexto donde el uso masivo de datos es una realidad cotidiana, desde las redes sociales hasta las plataformas de comercio electrónico, la información personal se ha convertido en un recurso valioso y vulnerable a la vez. La reciente aprobación de la Ley Orgánica de Protección de Datos Personales en nuestro país busca responder a estos desafíos, pero su implementación efectiva depende del desarrollo de mecanismos claros de supervisión y sanción (Mora, 2021). Esta investigación pretende analizar tanto los aspectos positivos de la normativa como sus limitaciones, proponiendo posibles mejoras que fortalezcan el sistema de protección de datos en el país.

Finalmente, este estudio se justifica en la necesidad de asegurar que el desarrollo tecnológico no vaya en detrimento de los derechos fundamentales de las personas; la falta de un sistema sólido de protección de datos puede generar riesgos significativos para la privacidad de los individuos y la seguridad de sus datos personales.

CAPITULO II

2. MARCO TEÓRICO

2.1.Concepto y Naturaleza del Derecho a la Protección de Datos Personales

La protección de datos personales como un derecho fundamental se erige como un pilar que sirve para salvaguardar la dignidad y privacidad de las personas; este derecho, aunque vinculado históricamente al derecho a la privacidad, ha evolucionado para responder a la problemática actual de la sociedad digital.

El derecho de protección de datos personales puede definirse como la facultad de las personas para controlar el uso, acceso y tratamiento de su información personal, garantizando su integridad y confidencialidad. Según Bygrave, "la protección de datos personales implica un conjunto de normas que buscan equilibrar el poder entre las entidades que recopilan datos y los individuos, asegurando que estos últimos mantengan el control sobre su información". (Bygrave, 2014)

Por su parte, Ferreres enfatiza que "el derecho a la protección de datos no solo se limita a la privacidad, sino que constituye un derecho autónomo que busca garantizar la autodeterminación informativa de las personas" (Ferreres, 2016). En esta línea, el autor subraya que el derecho no solo protege la información en sí, sino también las decisiones individuales respecto a cómo y cuándo compartirla.

De igual manera, González Fuster considera que "el derecho a la protección de datos personales es una respuesta jurídica a los riesgos asociados a la recopilación masiva de información en contextos digitales, donde los datos se han convertido en una herramienta de poder económico y político" (González, 2014). Así, se reconoce que la protección de datos tiene una función no solo individual, sino también social, al preservar la equidad en las relaciones entre ciudadanos y entidades.

2.2. Naturaleza del Derecho de Protección de Datos

La naturaleza del derecho a la protección de datos personales se puede entender desde tres perspectivas principales:

a) Derecho Fundamental Autónomo:

Como destaca Ferreres (2016), este derecho ha alcanzado autonomía en muchas jurisdicciones, siendo reconocido como un derecho fundamental separado del derecho a la privacidad; se ha consolidado como una categoría jurídica independiente. Además; Ferreras (2016) señala que este derecho no es una mera extensión del derecho a la privacidad, sino que responde a la necesidad de garantizar la autodeterminación informativa en un contexto de recopilación y procesamiento masivo de datos. Así, este derecho se diferencia al centrarse en el control que los individuos ejercen sobre el uso de su información.

La Unión Europea ha liderado este reconocimiento con el Reglamento General de Protección de Datos (GDPR), que en su artículo 1 establece explícitamente la protección de los datos personales como un derecho fundamental. Este modelo ha influido significativamente en legislaciones de todo el mundo, incluyendo al estado ecuatoriano que en la Constitución de 2008 reconoce explícitamente este derecho.

Aunque su reconocimiento como derecho fundamental es un avance significativo, la protección de datos personales se enfrenta a varios nudos críticos e importantes al momento de su implementación. González Fuster (2014) destaca que la autonomía de este derecho no debe ser solo nominal, sino que requiere mecanismos efectivos para su protección, incluyendo órganos reguladores fuertes y políticas públicas adecuadas.

La autonomía del derecho a la protección de datos personales tiene implicaciones profundas en la sociedad digital; puesto que; por un lado, garantiza la capacidad de los

individuos para decidir cómo se utiliza su información, lo que es esencial en un contexto donde los datos son una moneda de cambio clave en las interacciones económicas y sociales. Por otro lado, fortalece la confianza en las instituciones públicas y privadas, al establecer límites claros sobre el uso de la información personal.

b) Instrumento de Control y Autodeterminación Informativa:

La autodeterminación informativa, según Bygrave (2014), implica "el derecho de los individuos a determinar por sí mismos el destino de su información personal". Este principio nació en la jurisprudencia alemana, específicamente en el Caso del Censo de Población (1983), donde el Tribunal Constitucional Federal estableció que el control sobre los datos personales es esencial para preservar la dignidad humana y la libertad individual; describe la naturaleza del derecho a la protección de datos como una herramienta que permite a los individuos ejercer control sobre su información personal en un mundo dominado por tecnologías que facilitan la recopilación y procesamiento masivo de datos.

Ferreres (2016) sostiene que la autodeterminación informativa no solo garantiza el control sobre los datos personales, sino que también permite a las personas participar de manera activa en la construcción de su identidad digital, un aspecto crucial en la sociedad de la información. En este sentido, este principio va más allá de la privacidad, estableciendo un marco jurídico para gestionar la relación entre individuos y entidades que recopilan sus datos.

c) Mecanismo de Equidad Digital:

González Fuster (2014) argumenta que la protección de datos también debe ser vista como una herramienta para garantizar la equidad en la era digital, evitando que las brechas de información entre los actores se conviertan en un instrumento de dominación.

La relevancia de este derecho radica en su capacidad para mitigar los riesgos asociados al tratamiento indebido de datos personales, como la discriminación, el abuso de poder y las violaciones a la privacidad. Además, conforme a las consideraciones actuales, donde los datos se consideran "el nuevo petróleo", su protección es esencial para garantizar un equilibrio entre el desarrollo económico y la protección de los derechos individuales.

La protección de datos personales se fundamenta en la idea de que cada individuo tiene control sobre su información; este principio está reconocido en tratados internacionales, como el Pacto Internacional de Derechos Civiles y Políticos (Art. 17), y en normativa regional como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea han servido como modelos de regulación.

El derecho a la protección de datos personales aparece como una respuesta a los avances tecnológicos que permiten la recolección, procesamiento y almacenamiento de grandes cantidades de información; en América Latina, el desarrollo de leyes en esta materia ha sido reciente pero acelerado. En Ecuador, la Constitución de 2008 ya reconocía explícitamente este derecho en su artículo 66, numeral 19, donde se establece que los ciudadanos tienen el derecho a acceder, actualizar y eliminar su información personal. Sin embargo, la aparición de tecnologías avanzadas, como la inteligencia artificial y el big data, ha impulsado la creación de una legislación más detallada, como lo refleja la Ley Orgánica de Protección de Datos Personales (Romero, 2021).

Este derecho se fundamenta en la necesidad de salvaguardar la privacidad de los individuos frente al tratamiento de su información en un mundo cada vez más digitalizado. En Ecuador, la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en 2021 marca un hito en la defensa de este derecho; dando un paso significativo hacia la consolidación de un régimen jurídico que protege los datos personales; la ley

establece principios como la transparencia, finalidad, proporcionalidad y responsabilidad proactiva, los cuales alinean el sistema legal ecuatoriano con estándares internacionales.

Uno de los elementos más destacados de la Ley Orgánica de Protección de Datos Personales es la creación de la Superintendencia de Protección de Datos, encargada de velar por el cumplimiento de las normas y de promover una cultura de respeto a los derechos digitales; sin embargo pese a los avances normativos, la implementación efectiva del derecho a la protección requiere de mecanismos para su fortalecimiento; puesto que, muchos ciudadanos desconocen sus derechos y las medidas disponibles para proteger su información.

Actualmente las empresas y entidades tanto públicas como privadas deben adoptar sistemas que cumplan con las exigencias legales, lo que implica una inversión significativa en tecnología y capacitación, lo que es urgente para que se efectivice el contenido normativo y se proteja este derecho fundamental de los ciudadanos. Es de conocimiento público que actualmente se ha dado un incremento de ciberataques y es aquí donde esta uno de los graves problemas por los que se evidencia la importancia de proteger las bases de datos mediante medidas técnicas eficaces.

2.3.Importancia de la Protección de Datos en la Era Digital

La protección de los datos personales es más relevante que nunca debido a la creciente interconexión global y al uso generalizado de tecnologías digitales en prácticamente todos los aspectos de la vida cotidiana; desde la banca en línea hasta las redes sociales, los ciudadanos se enfrentan a múltiples escenarios donde sus datos pueden ser recopilados, analizados y compartidos. En este sentido, la legislación ecuatoriana desde la Constitución y la Ley Orgánica de Protección de Datos Personales establecen un marco legal que permite a las personas tener control sobre su información, reduciendo el riesgo de

violaciones a la privacidad y garantizando la protección frente a usos indebidos de sus datos personales.

La protección de datos no solo es esencial para salvaguardar la privacidad, sino también para preservar la confianza en las plataformas digitales; una regulación adecuada del tratamiento de datos contribuye a crear un entorno más seguro y transparente, lo que facilita la participación de los ciudadanos en la economía digital sin temor a que su información personal sea vulnerada.

El derecho a la protección de datos es un eje crucial para garantizar la dignidad y privacidad en un mundo digitalizado. Si bien Ecuador ha avanzado significativamente en términos legislativos, la verdadera protección dependerá de la educación ciudadana, la inversión tecnológica y una vigilancia efectiva por parte de las autoridades. La consolidación de este derecho no solo fortalece el marco democrático del país, sino que también protege a sus ciudadanos de los riesgos inherentes a la era de la información

2.4.El valor de los datos personales en la era digital

La era digital ha transformado la forma en que se generan, recopilan y procesan los datos personales; este entorno, impulsado por tecnologías como la inteligencia artificial, el big data y el internet de las cosas, presenta tanto oportunidades como riesgos latentes para los derechos de las personas; razón por la que, la protección de datos se convierte en un derecho fundamental para garantizar la privacidad, la seguridad y la autodeterminación informativa.

Los datos personales son, en la actualidad, un recurso valioso que sustenta gran parte de la economía digital. Según Bygrave (2014), "los datos personales son el nuevo petróleo de la economía global, utilizados para personalizar servicios, dirigir campañas de

marketing y desarrollar inteligencia artificial". Sin embargo, su explotación desmedida plantea riesgos como la pérdida de privacidad, la discriminación y la vigilancia masiva.

Ferreres (2016) señala que en la sociedad digital los individuos generan constantemente datos, ya sea a través de redes sociales, aplicaciones móviles o dispositivos conectados. En este escenario, garantizar la protección de estos datos es esencial no solo para preservar la privacidad, sino también para proteger la dignidad y libertad de las personas frente a su posible manipulación.

González Fuster (2014) argumenta que este derecho es esencial para garantizar la autodeterminación informativa, un principio que permite a las personas construir su identidad en la era digital sin el riesgo de interferencias indebidas.

La era digital plantea desafíos únicos para la protección de datos personales:

Ciberseguridad: El aumento de ciberataques y filtraciones de datos compromete la seguridad de la información personal; según estudios recientes, la exposición de datos sensibles puede derivar en robo de identidad y fraudes financieros.

Vigilancia Masiva: Tecnologías como el reconocimiento facial y el seguimiento en línea han incrementado la capacidad de las entidades públicas y privadas para vigilar a los individuos, lo que pone en riesgo derechos fundamentales como la privacidad.

Asimetrías de Poder: Las grandes empresas tecnológicas controlan una cantidad significativa de datos personales, lo que les otorga un poder desproporcionado frente a los usuarios. Este fenómeno, descrito por Bygrave (2014), enfatiza la necesidad de regulaciones estrictas para equilibrar esta relación.

La protección de datos tiene un impacto significativo en varios aspectos de la sociedad; así como una adecuada protección de datos fortalece la confianza de los

ciudadanos en las instituciones públicas y privadas. Según Ferreres (2016), "la transparencia en el manejo de datos es clave para fomentar la confianza en la economía digital".

La protección de datos es fundamental para prevenir abusos como la discriminación basada en datos sensibles y garantizar la igualdad de oportunidades en contextos como el empleo y la educación. Un entorno regulado que garantice la seguridad de los datos personales fomenta la innovación y la participación en la economía digital, al reducir los riesgos asociados con el intercambio de información.

2.5.Principios de Licitud

El principio de licitud es un fundamento esencial en la regulación del tratamiento de datos personales; establece que toda actividad relacionada con la recopilación, procesamiento y almacenamiento de datos debe cumplir con las leyes aplicables y respetar los derechos fundamentales de las personas. Este principio, recogido en normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos Personales (LOPDP), actúa como un mecanismo de garantía frente a posibles abusos en la era digital.

Se constituye como uno de los pilares fundamentales en el marco jurídico que regula la protección de los datos personales; en la era digital, donde la recolección y tratamiento de información son actividades cotidianas, este principio garantiza que el manejo de los datos personales se realice de manera legal, respetando los derechos fundamentales de los titulares de la información. En América Latina, los países han avanzado en la implementación de legislaciones que protegen este derecho, inspirados en marcos normativos internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

El principio de licitud establece que el tratamiento de datos personales debe realizarse con apego a la ley, es decir, debe estar sustentado en una base jurídica clara y legítima. El fundamento principal de este principio radica en que el uso de los datos personales solo es válido si existe una justificación legal o el consentimiento del titular (González, 2021). En este sentido, el principio de licitud actúa como una salvaguardia frente a la explotación indebida de la información personal, previniendo que los datos sean tratados de manera arbitraria o sin el conocimiento de los ciudadanos.

Para que el tratamiento de datos sea considerado lícito, debe cumplir con al menos una de las siguientes bases: el consentimiento del titular, el cumplimiento de una obligación legal, el interés legítimo del responsable del tratamiento, o la protección de intereses vitales de la persona (Mendoza, 2020). En ausencia de estas bases, el tratamiento de los datos carece de legitimidad y puede considerarse una violación de los derechos del titular.

El principio de licitud, según Bygrave (2014), establece que el tratamiento de datos personales solo puede realizarse cuando esté basado en un marco legal válido y legítimo; lo que obviamente incluye, entre otros aspectos, el consentimiento informado de los titulares de los datos o la existencia de un interés legítimo justificado por parte del responsable del tratamiento.

De acuerdo con Ferreres (2016), el principio de licitud no solo exige conformidad con las leyes nacionales e internacionales, sino también con principios éticos que resguarden la dignidad humana; este principio se articula con otros principios de protección de datos, como la transparencia y la proporcionalidad, para garantizar un tratamiento adecuado y respetuoso de la información personal.

La aplicación del principio de licitud requiere que los responsables del tratamiento de datos evalúen cuidadosamente las bases legales que sustentan sus actividades. González Fuster (2014) argumenta que la licitud no solo se refiere a la existencia de un marco normativo, sino también a la capacidad de demostrar que dicho marco ha sido respetado en cada etapa del tratamiento.

En el caso del consentimiento, por ejemplo, este debe ser otorgado de manera libre, específica, informada e inequívoca, tal como lo exige el GDPR (Art. 4) y la LOPDP de Ecuador (Art. 7). Esto significa que el consentimiento no puede ser obtenido mediante coerción, omisiones o interpretaciones ambiguas. Otro ejemplo relevante es el uso de datos personales en investigaciones científicas o fines estadísticos; en estos casos, el principio de licitud exige que los datos sean anonimizados o se utilicen medidas de minimización para garantizar la protección de los derechos de los titulares.

El principio de licitud adquiere una relevancia particular en la era digital, donde el tratamiento masivo y automatizado de datos plantea riesgos significativos para la privacidad y otros derechos fundamentales. Según Bygrave (2014), la licitud actúa como una barrera frente a prácticas abusivas, como la recopilación indiscriminada de datos o su uso con fines distintos a los autorizados.

Ferreres (2016) destaca que este principio es clave para garantizar la confianza en las instituciones públicas y privadas que manejan datos personales; actualmente las violaciones de datos son cada vez más comunes, la adherencia al principio de licitud no solo protege a los individuos, sino que también fortalece la legitimidad de las organizaciones responsables.

En Ecuador, el principio de licitud ha sido instrumental para consolidar un marco normativo que regule el tratamiento de datos en sectores sensibles como la salud, la

educación y el comercio electrónico. La Superintendencia de Protección de Datos Personales, creada bajo la LOPDP, supervisa el cumplimiento de este principio y aplica sanciones en casos de incumplimiento.

Además, González Fuster (2014) señala que las tecnologías emergentes, como la inteligencia artificial y el big data, complican la evaluación de la licitud, dado que sus procesos automatizados pueden superar las capacidades de regulación y supervisión tradicionales.

El principio de licitud es un pilar esencial de la protección de datos personales, que garantiza que el tratamiento de información se realice dentro de un marco legal y ético; en la actual era digital, su correcta aplicación es fundamental para proteger los derechos de las personas y fomentar la confianza en las instituciones. Sin embargo, su efectividad depende de un esfuerzo conjunto entre reguladores, responsables del tratamiento y ciudadanos, quienes deben ser conscientes de la importancia de este principio para la construcción de una sociedad más justa y equitativa.

2.6.Principio de transparencia

El principio de transparencia es uno de los pilares fundamentales del derecho a la protección de datos personales, ya que garantiza que las personas tengan acceso claro y comprensible a la información sobre cómo se recopilan, procesan y utilizan sus datos. Este principio, ampliamente reconocido en normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y en legislaciones nacionales como la Ley Orgánica de Protección de Datos Personales (LOPDP), busca empoderar a los individuos y promover la confianza en las instituciones que manejan datos personales.

El principio de transparencia se fundamenta en la obligación de los responsables del tratamiento de datos de proporcionar información clara, accesible y comprensible sobre

las actividades relacionadas con los datos personales. Según Bygrave (2014), "la transparencia implica no solo informar a los individuos sobre el uso de sus datos, sino también garantizar que esta información sea fácilmente comprensible y accesible para cualquier persona".

En el marco del GDPR, el principio de transparencia se encuentra reflejado en los artículos 12 a 14, que establecen requisitos específicos sobre cómo debe proporcionarse la información a los titulares de los datos. De manera similar, la LOPDP de Ecuador, promulgada en 2021, estipula que los responsables del tratamiento deben informar de forma clara sobre el propósito, la base legal y los derechos de los titulares, entre otros aspectos.

Ferreres (2016) destaca que este principio no solo cumple una función informativa, sino también preventiva, al reducir la asimetría de información entre los responsables del tratamiento y los titulares de los datos. La implementación del principio de transparencia requiere que las organizaciones adopten prácticas que permitan a los titulares de datos comprender y controlar el uso de su información. Esto incluye:

Políticas de Privacidad Claras y Accesibles

Las políticas de privacidad deben estar redactadas en un lenguaje sencillo, evitando tecnicismos que dificulten su comprensión. Según González Fuster (2014), "la transparencia exige que las políticas no solo sean comprensibles, sino también accesibles, disponibles en los idiomas pertinentes y adaptadas a las capacidades del público objetivo".

Notificaciones sobre el Tratamiento de Datos

El principio de transparencia obliga a los responsables a informar previamente a los titulares sobre el tratamiento de sus datos, incluyendo el propósito, la duración, los destinatarios y las posibles transferencias internacionales.

Derechos de Acceso y Rectificación

La transparencia también implica garantizar que los titulares puedan acceder fácilmente a sus datos, conocer el estado de su tratamiento y corregir cualquier inexactitud.

Supervisión Regulatoria y Buenas Prácticas

Por ejemplo en Ecuador, la Superintendencia de Protección de Datos Personales supervisa el cumplimiento del principio de transparencia y promueve prácticas responsables en el manejo de datos personales.

En la era digital, donde el uso masivo de datos personales es una práctica común, la transparencia adquiere un papel esencial para salvaguardar la confianza entre ciudadanos e instituciones. Bygrave (2014) argumenta que "la transparencia es esencial para mitigar el riesgo de abuso de poder y garantizar que los titulares mantengan el control sobre sus datos".

Ferreres (2016) destaca que, sin transparencia, los titulares de los datos quedan en una posición de desventaja frente a entidades que poseen vastas capacidades tecnológicas para procesar y analizar su información. Además, la falta de transparencia puede generar desconfianza y conflictos legales, especialmente en sectores sensibles como la banca, la salud y las redes sociales.

En América Latina, varios países han desarrollado legislaciones de protección de datos personales que incorporan el principio de transparencia como uno de sus fundamentos principales; en México, por ejemplo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares obliga a las empresas a informar de manera clara a los titulares de los datos sobre el tratamiento que se dará a su información personal (Mendoza, 2020). De igual manera, en Argentina, la Ley de Protección de Datos Personales garantiza el derecho de los ciudadanos a conocer cómo se procesan sus datos y a qué entidades se les puede proporcionar (González, 2021). En el contexto ecuatoriano, la LOPDP promueve la transparencia como un medio para fortalecer la relación entre ciudadanos y organizaciones, fomentando un uso ético y responsable de los datos personales.

El principio de transparencia es fundamental en la protección de los datos personales, ya que garantiza que los titulares de la información conozcan de manera clara y accesible cómo, por qué y quién gestiona sus datos; este principio asegura que las personas tengan control sobre el tratamiento de su información personal y puedan tomar decisiones informadas. Además; establece que el tratamiento de los datos personales debe ser accesible y comprensible para los titulares de la información; lo que implica que los responsables del tratamiento de datos deben proporcionar información clara, precisa y fácilmente entendible sobre el uso que darán a los datos, los fines del tratamiento, y los derechos que los titulares pueden ejercer sobre su información (Maldonado, 2020). Este principio busca eliminar la opacidad en el manejo de los datos personales, evitando que las personas desconozcan cómo se utiliza su información o que sea tratada para fines no consentidos.

Uno de los elementos clave del principio de transparencia es la obligación de las empresas e instituciones de informar a los titulares sobre la identidad del responsable del

tratamiento, los datos que se recopilan, la finalidad del procesamiento, el plazo de conservación y los derechos que el titular puede ejercer, como el acceso, rectificación, cancelación u oposición (Gómez, 2021). La claridad y accesibilidad de esta información es esencial para garantizar que el tratamiento de los datos sea legítimo y que los titulares puedan actuar en defensa de sus derechos.

El principio de transparencia es un mecanismo que facilita el control de los titulares sobre sus datos personales; el conocimiento detallado sobre cómo se procesan sus datos permite que las personas ejerzan sus derechos de manera efectiva. En este sentido, la transparencia no solo implica que las empresas o instituciones cumplan con su deber de informar, sino también que los ciudadanos tengan acceso a la información necesaria para tomar decisiones conscientes sobre el uso de sus datos (Romero, 2021).

Un ejemplo claro de cómo se materializa este principio en la práctica es a través de las políticas de privacidad, que deben ser fácilmente comprensibles y accesibles; estas políticas deben explicar claramente qué datos se recolectan, con qué finalidad y si se compartirán con terceros. La transparencia en el manejo de la información fortalece la confianza entre los usuarios y las entidades que tratan sus datos, ya sean públicas o privadas.

La Ley Orgánica de Protección de Datos Personales, promulgada en 2021, también consagra el principio de transparencia como uno de los pilares fundamentales del tratamiento de datos; esta ley obliga a las entidades responsables a proporcionar a los titulares información clara, precisa y en un lenguaje comprensible sobre el uso de sus datos personales (Romero, 2021). Además, garantiza que los ciudadanos puedan acceder a sus datos y corregir o eliminar la información si consideran que se ha manejado de manera incorrecta.

2.7.El derecho a la Protección de datos como instrumento de control

El derecho a la protección de datos se configura como un instrumento de control al proporcionar a los ciudadanos herramientas legales para supervisar y limitar el uso de su información personal. La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, establece principios como transparencia, minimización de datos y finalidad específica, que buscan garantizar que los datos personales se utilicen de manera adecuada y proporcional; así por ejemplo la creación de autoridades de control, como la Superintendencia de Protección de Datos Personales en Ecuador, refuerza el ejercicio de la autodeterminación informativa al garantizar que las entidades cumplan con las normativas y sancionando posibles infracciones.

Según González Fuster (2014), "los derechos de acceso, rectificación, oposición y olvido son pilares fundamentales del control informativo". Estos derechos permiten a los individuos corregir errores, retirar consentimientos y exigir la eliminación de datos obsoletos o irrelevantes.

La autodeterminación informativa en la sociedad digital, es muy importante en un mundo donde los datos personales se han convertido en un activo económico, puesto que no solo protege la privacidad, sino que también equilibra las relaciones de poder entre individuos y corporaciones. Bygrave (2014) argumenta que "la protección de datos permite a los ciudadanos negociar las condiciones bajo las cuales sus datos son utilizados, promoviendo una economía digital más justa y ética".

Sin embargo, Ferreres (2016) advierte que la implementación efectiva de este control enfrenta desafíos significativos, como la falta de educación ciudadana y la asimetría tecnológica entre los titulares de los datos y las grandes empresas tecnológicas. Además, el creciente uso de tecnologías como inteligencia artificial y big data plantea

nuevos riesgos para la autodeterminación informativa, al automatizar procesos de recopilación y análisis de datos.

El derecho a la protección de datos personales, como instrumento de control y expresión de la autodeterminación informativa, es fundamental en la era digital; permite a los individuos ejercer su autonomía y proteger su dignidad en un contexto donde los datos son objeto de constante recopilación y explotación. Sin embargo, su efectividad depende de un equilibrio entre normativas sólidas, supervisión institucional y educación ciudadana, garantizando así que este derecho cumpla su función como pilar de las democracias modernas.

El derecho a la protección de datos establecido en un marco normativo en la legislación ecuatoriana se constituye como un instrumento de control al proporcionar a los ciudadanos herramientas legales para supervisar y limitar el uso de su información personal. Estas herramientas incluyen:

Principios de Tratamiento de Datos

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, promulgada en 2021, establece principios como transparencia, minimización de datos y finalidad específica, que buscan garantizar que los datos personales se utilicen de manera adecuada y proporcional.

2.8.Derechos de los Titulares de Datos

Según González Fuster (2014), "los derechos de acceso, rectificación, oposición y olvido son pilares fundamentales del control informativo". Estos derechos permiten a los individuos corregir errores, retirar consentimientos y exigir la eliminación de datos obsoletos o irrelevantes.

2.9.Supervisión Regulatoria

La creación de autoridades de control, como la Superintendencia de Protección de Datos Personales en Ecuador, refuerza el ejercicio de la autodeterminación informativa al garantizar que las entidades cumplan con las normativas y sancionando posibles infracciones.

El derecho a la protección de datos personales, como instrumento de control y expresión de la autodeterminación informativa, es fundamental en la era digital; permite a los individuos ejercer su autonomía y proteger su dignidad en una realidad actual donde los datos son objeto de constante recopilación y explotación. Sin embargo, su efectividad depende de un equilibrio entre normativas sólidas, supervisión institucional y educación ciudadana, garantizando así que este derecho cumpla su función como pilar de las democracias modernas.

2.10. Derechos de los Titulares de los Datos

En la era digital, el tratamiento masivo de datos personales exige establecer mecanismos firmes y seguros para la protección de los derechos individuales; ante esta realidad, los derechos de los titulares de datos personales son una herramienta esenciales para garantizar el control y la autodeterminación informativa. Estos derechos, reconocidos en normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y en legislaciones nacionales como la Ley Orgánica de Protección de Datos Personales (LOPDP), buscan equilibrar las relaciones entre los titulares y los responsables del tratamiento de datos.

Los derechos de los titulares de datos son prerrogativas legales que permiten a los individuos controlar el tratamiento de su información personal. Según Bygrave (2014),

estos derechos son "expresiones del principio de autodeterminación informativa, diseñadas para empoderar a los individuos en un entorno dominado por el manejo masivo de datos".

En el contexto del Reglamento General de la Protección de Datos (2016), estos derechos incluyen, entre otros, el acceso, rectificación, supresión, portabilidad y oposición. La Ley Orgánica de Protección de Datos Personales adopta un enfoque similar, reconociendo una amplia gama de derechos destinados a proteger la privacidad y garantizar la transparencia en el tratamiento de datos personales.

Ferreres (2016) destaca que la existencia de estos derechos no solo protege la privacidad individual, sino que también fortalece la confianza en las instituciones públicas y privadas que manejan información personal. Los principales derechos de los titulares de datos; son:

Derecho de Acceso: Este derecho permite a los titulares obtener información sobre el tratamiento de sus datos, incluyendo la finalidad, la base legal y los destinatarios. Según González Fuster (2014), "el derecho de acceso es el fundamento de todos los demás derechos, ya que permite a los individuos conocer y evaluar cómo se utiliza su información".

Derecho de Rectificación: Los titulares tienen el derecho de corregir errores o actualizar su información personal. La LOPDP, en su Artículo 12, establece que los responsables deben atender estas solicitudes de manera eficiente y gratuita.

Derecho de Supresión o "Derecho al Olvido": Este derecho permite a los individuos solicitar la eliminación de sus datos cuando ya no son necesarios para los fines para los que fueron recopilados. En el contexto digital, esto incluye la eliminación de información de motores de búsqueda y redes sociales.

Derecho a la Portabilidad de Datos: Reconocido por primera vez en el GDPR, este derecho permite a los titulares recibir sus datos en un formato estructurado y transferirlos a otro proveedor. Este mecanismo promueve la competencia y protege la autonomía del usuario.

Derecho de Oposición: Los titulares pueden oponerse al tratamiento de sus datos en ciertos casos, como el marketing directo o el procesamiento basado en intereses legítimos.

Derecho a la Limitación del Tratamiento: Este derecho permite a los individuos restringir temporalmente el uso de sus datos mientras se resuelven disputas relacionadas con su tratamiento.

Derecho a no ser objeto de decisiones automatizadas: Este derecho protege a los titulares de ser evaluados exclusivamente mediante algoritmos, garantizando la intervención humana en decisiones que afecten significativamente sus derechos.

Los derechos de los titulares son fundamentales para garantizar la equidad, transparencia y seguridad en el tratamiento de datos personales. Bygrave (2014) argumenta que estos derechos son esenciales para equilibrar las relaciones de poder entre los titulares y las entidades que procesan sus datos, especialmente en un entorno donde las asimetrías tecnológicas son comunes.

Ferreres (2016) destaca que el ejercicio de estos derechos no solo protege la privacidad individual, sino que también fomenta la responsabilidad de los responsables del tratamiento, promoviendo un uso ético y legal de los datos personales.

En el caso ecuatoriano, la Ley Orgánica de Protección de Datos Personales ha fortalecido la protección de los titulares al establecer procedimientos claros para el

ejercicio de estos derechos y sanciones para las entidades que los vulneren. Los derechos de los titulares de datos son una pieza clave en el marco de la protección de datos personales, al empoderar a los individuos y garantizar la transparencia en el tratamiento de su información; en última instancia, estos derechos no solo protegen la privacidad, sino que también fortalecen la confianza en las instituciones y promueven un entorno digital más justo y equitativo.

La LOPDP garantiza a los titulares de los datos personales derechos fundamentales como el acceso, rectificación, cancelación y oposición al tratamiento de sus datos. También reconoce el derecho a la portabilidad de los datos y a la limitación del tratamiento en ciertos casos (Art. 11, LOPDP). Estos derechos permiten que los ciudadanos mantengan el control sobre su información personal en el entorno digital.

2.11. Derecho a la Intimidad y a la Privacidad

El derecho a la intimidad y la privacidad es uno de los derechos fundamentales más relevantes en la actualidad, dado el impacto de las tecnologías de la información y la comunicación en la vida de las personas; estos derechos protegen a los individuos contra la intromisión no autorizada en su vida personal, tanto por parte de otros individuos como de entidades públicas y privadas.

El derecho a la intimidad protege a las personas contra cualquier forma de intrusión no consentida en su vida privada; este derecho garantiza la protección de aspectos personales como la correspondencia, las comunicaciones, la información personal y los espacios privados, los cuales no deben ser objeto de vigilancia o manipulación sin una causa justificada y el debido consentimiento (González, 2021). Por su parte, el derecho a la privacidad tiene un enfoque más amplio y está relacionado con el control que cada

individuo tiene sobre sus datos personales y la libertad de decidir qué información comparte con terceros (Mendoza, 2020).

En el ámbito internacional, el derecho a la privacidad está consagrado en varios instrumentos, como la Declaración Universal de Derechos Humanos de 1948, cuyo artículo 12 establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia" (Naciones Unidas, 1948). Asimismo, en la región latinoamericana, la Convención Americana sobre Derechos Humanos también reconoce este derecho en su artículo 11 (OEA, 1969).

En América Latina, los derechos a la intimidad y la privacidad han sido reconocidos y protegidos en las constituciones nacionales de varios países. En Ecuador, la Constitución de 2008 garantiza el derecho a la privacidad e intimidad personal y familiar, así como la protección de los datos personales (Constitución de la República del Ecuador, 2008). De manera similar, en México, la Constitución reconoce el derecho a la privacidad y protege las comunicaciones privadas de cualquier intervención no autorizada (Constitución Política de los Estados Unidos Mexicanos, 1917).

Sin embargo, más allá de las constituciones, varios países han avanzado en la promulgación de leyes específicas que regulan el tratamiento de los datos personales y la protección de la intimidad en el contexto digital. La Ley Orgánica de Protección de Datos Personales en Ecuador, por ejemplo, busca garantizar que el tratamiento de datos personales se realice respetando la privacidad de los individuos y sus derechos fundamentales (Romero, 2021). En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece las bases para que las personas puedan ejercer control sobre la información que las identifica (Gómez, 2021).

Con la llegada de la era digital, el derecho a la intimidad y la privacidad ha sido sometido a tensiones sin precedentes; la proliferación de plataformas digitales, redes sociales y tecnologías de recolección masiva de datos ha permitido la creación de perfiles detallados de los usuarios a través de la recopilación, almacenamiento y procesamiento de grandes cantidades de información personal (Maldonado, 2020). En este nuevo entorno, las empresas tecnológicas tienen acceso a datos sensibles como la ubicación, hábitos de consumo, preferencias políticas e incluso datos biométricos.

La preocupación por la privacidad ha crecido a medida que estas tecnologías se han vuelto omnipresentes, y los ciudadanos muchas veces no son conscientes de la magnitud de la información que comparten y cómo se utiliza. Los algoritmos de inteligencia artificial y el big data pueden ser empleados para realizar predicciones y generar decisiones automatizadas, lo que pone en riesgo la privacidad de las personas (González, 2021). En este sentido, las leyes de protección de datos se vuelven esenciales para garantizar que las empresas y gobiernos respeten la intimidad de los usuarios y no hagan un uso indebido de su información.

2.12. Derecho al consentimiento informado

Es un principio fundamental en diversas áreas, como la salud, la investigación y el tratamiento de datos personales; garantiza que una persona pueda tomar decisiones libres y conscientes sobre su cuerpo, su salud o su información personal, después de haber recibido toda la información relevante de manera comprensible.

El consentimiento informado es un principio esencial en la protección de datos personales, que otorga a los titulares el control sobre cómo y por qué se utiliza su información; este derecho permite a los individuos decidir, de manera libre e informada, el tratamiento de sus datos personales, promoviendo la transparencia y el respeto a su

autodeterminación informativa. Reconocido en normativas como el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, el consentimiento informado actúa como un pilar de las relaciones entre los responsables del tratamiento y los titulares de datos.

El consentimiento informado se define como la autorización libre, específica, informada e inequívoca otorgada por un individuo para el tratamiento de sus datos personales. Según Bygrave (2014), el consentimiento es "una expresión del principio de autonomía individual, que permite a los titulares de datos ejercer control sobre sus derechos en el ámbito de la protección de datos".

El Reglamento General de Protección de Datos, en su artículo 4(11), establece que el consentimiento debe ser explícito y verificable, garantizando que los titulares comprendan plenamente las implicaciones del tratamiento de sus datos. La Ley Orgánica de Protección de Datos, en su artículo 7, refuerza esta visión al exigir que el consentimiento sea previo, específico, informado y libre de cualquier tipo de coerción.

El consentimiento informado se refiere al proceso por el cual una persona da su autorización para realizar un tratamiento médico, participar en una investigación o permitir el uso de sus datos personales, tras recibir información adecuada y comprensible sobre los riesgos, beneficios y consecuencias de dicha acción (González, 2021). Este proceso es esencial para asegurar que las personas puedan tomar decisiones autónomas sobre aspectos que afectan su vida y bienestar.

Para que el consentimiento informado sea válido, debe cumplir con varios requisitos: debe ser libre, específico, informado y explícito; la persona debe tener libertad para dar o negar su consentimiento sin presiones; debe estar bien informada sobre lo que implica el proceso o tratamiento, y el consentimiento debe ser dado de manera clara y

voluntaria (Mendoza, 2020). Además, el consentimiento puede ser revocado en cualquier momento sin consecuencias negativas para el individuo.

El consentimiento informado juega un rol crucial en la protección de los datos personales. En la era digital, donde la recolección y el tratamiento de datos son omnipresentes, las personas deben ser informadas sobre el uso que se hará de su información personal y deben tener la opción de aceptar o rechazar dicho tratamiento. En este contexto, el consentimiento debe ser explícito, informado y específico para cada finalidad de tratamiento (Gómez, 2021).

La Ley Orgánica de Protección de Datos Personales (2021) establece que el tratamiento de datos personales solo puede realizarse si el titular ha otorgado su consentimiento libre, específico, informado y claro; además, los titulares tienen el derecho de revocar su consentimiento en cualquier momento, sin afectar la licitud del tratamiento previo a la revocación. Este marco legal protege a los ciudadanos de la recolección y uso indebido de su información personal, asegurando que el tratamiento de datos se realice con respeto a su autonomía y privacidad (Romero, 2021).

2.13. Requisitos para el Consentimiento Informado

Para que el consentimiento sea válido, debe cumplir con ciertos requisitos legales y éticos:

Libertad: El consentimiento debe otorgarse sin coacción, presión o condicionamientos indebidos. Esto significa que los titulares deben tener la opción real de negarse o retirar su consentimiento sin sufrir consecuencias adversas.

Especificidad: El tratamiento debe estar claramente definido, indicando la finalidad, los datos involucrados y los destinatarios de la información. Según Ferreres (2016), la especificidad asegura que el consentimiento no sea genérico ni ambiguo.

Información Clara y Accesible: Los responsables del tratamiento deben proporcionar información detallada y comprensible sobre el uso de los datos. La transparencia en la comunicación es clave para garantizar que los titulares comprendan las implicaciones del tratamiento.

Capacidad de Verificación: Los responsables deben ser capaces de demostrar que el consentimiento fue otorgado de manera válida, utilizando mecanismos de registro y documentación.

Revocabilidad: Los titulares tienen el derecho de retirar su consentimiento en cualquier momento, sin que esto afecte la licitud del tratamiento previo.

El consentimiento informado es fundamental para garantizar la autonomía de los titulares de datos y fomentar la confianza en las instituciones que manejan información personal. González Fuster (2014) argumenta que este derecho es "la base sobre la cual los titulares pueden ejercer un control real sobre sus datos, protegiendo su privacidad y dignidad en el entorno digital". Además, el consentimiento informado promueve la transparencia y la responsabilidad, obligando a los responsables del tratamiento a justificar sus acciones y garantizar el cumplimiento de las normativas aplicables.

Al ser parte del marco legal estatal la Ley Orgánica de Protección de Datos Personales en donde se da el reconocimiento del consentimiento informado; este hecho representa un avance hacia la protección efectiva de los derechos de los titulares de datos Este derecho es especialmente relevante en sectores como la salud, donde el tratamiento de datos sensibles requiere un nivel adicional de cuidado y respeto.

El consentimiento informado es un derecho clave en la protección de datos personales, que garantiza la autonomía y el control de los titulares sobre su información; su correcta implementación es fundamental para preservar la confianza en las instituciones y

proteger los derechos fundamentales, pero requiere una supervisión efectiva y un esfuerzo continuo para garantizar que el consentimiento sea verdaderamente libre, informado y significativo.

2.14. Mecanismos jurídicos establecidos en la Ley Orgánica de Protección de Datos Personales para la protección de datos personales

La Ley Orgánica de Protección de Datos Personales, promulgada en mayo de 2021, establece un marco normativo integral para proteger los datos personales de los ciudadanos; es esta inspirada en estándares internacionales como el Reglamento General de Protección de Datos de la Unión Europea; define principios, derechos y obligaciones relacionados con el tratamiento de datos personales, así como mecanismos jurídicos para garantizar su cumplimiento.

Se puede decir que los principales mecanismos jurídicos previstos en esta legislación:

2.15. Reconocimiento de Principios Rectores

La ley establece principios que guían el tratamiento de datos personales y aseguran la protección de los derechos de los titulares, entre los que destacan:

Licitud: El tratamiento de datos debe basarse en una base legal válida.

Transparencia: Los titulares deben recibir información clara y accesible sobre el uso de sus datos.

Minimización de Datos: Solo deben recopilarse los datos necesarios para cumplir con una finalidad específica.

Proporcionalidad: El tratamiento debe ser adecuado y pertinente en relación con los fines para los que se recaban.

Responsabilidad Proactiva: Los responsables deben garantizar el cumplimiento de las disposiciones legales de manera continua y efectiva.

2.16. Derechos de los Titulares de Datos

Se reconoce una amplia gama de derechos para los titulares, que son esenciales para garantizar la protección de sus datos personales:

Derecho de acceso: Permite a los titulares conocer qué datos se están procesando, con qué finalidad y por quién.

Derecho de rectificación: Permite corregir errores o actualizar información inexacta.

Derecho de supresión ("derecho al olvido"): Permite solicitar la eliminación de datos cuando estos ya no son necesarios o su tratamiento es ilícito.

Derecho a la portabilidad: Facilita la transferencia de datos entre diferentes responsables, en un formato estructurado y de uso común.

Derecho de oposición: Los titulares pueden negarse al tratamiento de sus datos por motivos específicos.

Derecho a no ser objeto de decisiones automatizadas: Protege contra evaluaciones realizadas exclusivamente mediante algoritmos, especialmente si tienen efectos significativos sobre la persona.

2.17. Obligaciones de los Responsables y Encargados del Tratamiento

La Ley Orgánica de Protección de Datos Personales establece deberes específicos para quienes manejan datos personales, garantizando que el tratamiento sea legal y seguro:

Registro de Actividades de Tratamiento (RAT): Los responsables deben mantener un registro detallado de las actividades de tratamiento realizadas.

Evaluaciones de Impacto en la Protección de Datos: Cuando se traten datos sensibles o se realicen tratamientos de alto riesgo, se requiere una evaluación previa para identificar y mitigar posibles impactos.

Notificación de Violaciones de Seguridad: En caso de incidentes que afecten la seguridad de los datos, los responsables deben informar a la autoridad competente y, si es necesario, a los titulares afectados.

Adopción de Medidas Técnicas y Organizativas: Los responsables deben implementar medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados, pérdida o destrucción.

2.18. Creación de la Superintendencia de Protección de Datos Personales

Uno de los avances más importantes de la Ley Orgánica de Protección de Datos Personales es la creación de la Superintendencia de Protección de Datos Personales, una entidad independiente encargada de supervisar el cumplimiento de la ley. Sus principales funciones incluyen:

Vigilar y sancionar el incumplimiento de la legislación.

Emitir directrices y normativas complementarias.

Resolver las denuncias presentadas por los titulares de datos.

Promover la cultura de protección de datos personales a través de campañas de educación y sensibilización.

2.19. Mecanismos de Protección y Denuncia

La ley establece procedimientos claros para que los titulares de datos puedan proteger sus derechos:

Habeas Data: Garantiza que los ciudadanos puedan acceder a sus datos personales, rectificarlos o solicitar su eliminación mediante un recurso judicial.

Procesos Administrativos: Los titulares pueden presentar quejas ante la Superintendencia de Protección de Datos en caso de violaciones a sus derechos.

c) Sanciones Administrativas: La ley contempla multas y otras medidas coercitivas para quienes incumplan con las disposiciones legales.

2.20. Regulación de Categorías Especiales de Datos

La Ley Orgánica de Protección de Datos Personales otorga una protección adicional a los datos sensibles, que incluyen información sobre salud, orientación sexual, origen étnico, religión, opiniones políticas, entre otros. Para su tratamiento, se requiere rigurosamente:

Consentimiento expreso y específico del titular.

Medidas de seguridad reforzadas para evitar filtraciones o usos indebidos.

2.20. Transferencia Internacional de Datos

La transferencia de datos personales hacia otros países está sujeta a condiciones estrictas para garantizar que los datos estén igualmente protegidos:

Solo se permite la transferencia a países que cuenten con un nivel adecuado de protección.

En ausencia de dicho nivel, se requieren garantías adicionales, como cláusulas contractuales específicas o la autorización de la Superintendencia.

2.21. Capacitación y Sensibilización

La Ley Orgánica de Protección de Datos Personales promueve la capacitación de responsables y encargados del tratamiento para fomentar una cultura de respeto hacia los derechos de los titulares y el cumplimiento de las normativas.

La ley establece un marco jurídico que prácticamente integra principios, derechos y obligaciones destinados a garantizar el tratamiento adecuado de los datos personales; los complementa con la creación de la Superintendencia de Protección de Datos Personales y la implementación de mecanismos específicos, esta legislación representa un avance significativo en la protección de los derechos de los ciudadanos en la era digital. Sin embargo, su efectividad dependerá de la capacidad de supervisión, la educación ciudadana y la voluntad de los responsables para adoptar prácticas responsables y transparentes.

CAPITILO III

3. METODOLOGÍA

3.1.Método de la Investigación

Método analítico: A través de este método, se descompondrán las leyes ecuatorianas relacionadas con la protección de los datos personales, como la Ley Orgánica de Protección de Datos Personales, para analizar su estructura, principios, alcance y efectividad. Además, se examinaron las obligaciones impuestas a las empresas y organismos que manejan datos personales y las sanciones establecidas por incumplimiento.

Método inductivo: Se empleó para observar casos concretos y prácticas en Ecuador en los que se hayan aplicado los mecanismos de protección de datos personales; a partir de estos ejemplos, se logró extraer conclusiones generales sobre la efectividad y la problemática que enfrenta la legislación ecuatoriana para adaptarse a las nuevas tecnologías.

Método deductivo: Con este método, se partirá de los principios generales del derecho de la privacidad y la protección de datos, establecidos tanto a nivel internacional como en la normativa ecuatoriana, para aplicarlos a la realidad ecuatoriana.

3.2.Tipo de Investigación

La investigación es descriptiva y explicativa.

Investigación descriptiva: Tiene como objetivo identificar y detallar los mecanismos jurídicos vigentes en la legislación ecuatoriana que regulan la protección de los datos personales. Se busca describir cómo se estructura este marco legal y las herramientas jurídicas disponibles para salvaguardar la privacidad de las personas en el entorno digital.

Investigación explicativa: Busca analizar las causas y efectos de la aplicación de estas normativas en la práctica; se explica cómo los avances tecnológicos han impactado en la legislación y de qué manera se aplican estas normativas para enfrentar los retos asociados a la protección de los datos personales en la era digital.

3.3.Técnicas e Instrumentos de Investigación

Las herramientas principales que se utilizaron para la recopilación de información y análisis fueron las siguientes:

Revisión bibliográfica y documental: Se realizo una exhaustiva revisión de las normativas nacionales ecuatorianas, tratados internacionales, jurisprudencia, informes de organismos especializados y estudios académicos relacionados con la protección de datos personales. La Ley Orgánica de Protección de Datos Personales el principal texto normativo para ser estudiado, junto con su interacción con otras normativas locales y regionales.

Entrevistas y encuestas: En base a cuestionarios previamente estructurados para ser aplicados con la finalidad de dilucidar dudas y esclarecer temáticas.

3.4.Criterio de Inclusión y Criterio de Exclusión

Se llevaron a cabo entrevistas a directores de tecnología de la información de dos instituciones públicas del Cantón Guaranda: Gobierno Descentralizado Autónomo de la Provincia de Bolívar y Director de Tecnologías de la Información de la Universidad Estatal de Bolívar; quienes con basto conocimiento aportaron a la presente investigación para esclarecer varios puntos importantes, pero por sobre todo dudas.

Para las encuestas fueron aplicadas a ciudadanos, para obtener perspectivas prácticas sobre la aplicación de las normativas y la problemática existente.

3.5.Población y Muestra

Entrevistas: 2 directores de Tecnología de la Información de dos instituciones públicas del Cantón Guaranda: Gobierno Descentralizado Autónomo de la Provincia de Bolívar y director de Tecnologías de la Información de la Universidad Estatal de Bolívar, Cantón Guaranda, Provincia de Bolívar.

Encuestas: 50 ciudadanos del sector urbano del cantón Guaranda, Provincia de Bolívar.

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

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1.Resultados

Entrevista

Entrevistados: 2 directores de Tecnología de la Información de dos instituciones públicas del Cantón Guaranda.

Entrevistado 1: Ing. Henry Albán

Entrevistado 2: Ing. Cristhian Agualongo

De las entrevistas realizadas podemos concluir:

Pregunta 1

¿Cuál es el marco legal vigente para la protección de los datos personales?

Entrevistado 1: Ley de Protección de Datos y Reglamento a la Protección de Datos. Desde 2020 es oficial y se viene desarrollando, El Esquema Gubernamental de Seguridad de la Información (EGSI) se aplica a nivel Gubernamental en las Instituciones.

Entrevistado 2: Ley de Protección de Datos y Reglamento de la Protección de Datos que se aplican en las Instituciones y ayuda a que no se filtren, adulterio o pierdan los datos personales.

Pregunta 2

¿Cómo se compara la Ley Orgánica de Protección de Datos Personales de 2021 con otros marcos normativos internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea?

Entrevistado 1: Es buena y permite proteger la integridad de los datos personales.

Entrevistado 2: Proteger y evitar perdida de datos, que no se vulnere y no se modifique el software, además un software adicional que se vaya mejorando con el paso del tiempo.

Pregunta 3

¿Qué principios y derechos fundamentales garantiza la legislación ecuatoriana en relación con la protección de los datos personales en el contexto de las Tecnología de la información?

Entrevistado 1: Derecho a la privacidad, seguridad de la información y responsabilidad en el manejo de datos personales.

Entrevistado 2: Da seguridad a la información, transparencia de datos y confiabilidad, se asegura el derecho a la privacidad.

Pregunta 4

¿Qué mecanismos de control y sanción establece la ley para prevenir y sancionar violaciones a la privacidad y el uso indebido de los datos personales?

Entrevistado 1: Diferentes tipos de sanciones previstas en la ley.

Entrevistado 2: En casos de suplantación de identidad puede llegar a ser sancionado con pena de cárcel.

Pregunta 5

¿Cómo se está implementando la Ley Orgánica de Protección de Datos Personales en las instituciones públicas y privadas de Ecuador?

Entrevistado 1: A nivel Nacional se vienen implementando en algunas instituciones antes que en otras. Existe el comité de seguridad de la información y un delegado de dicho comité, además de organizar reuniones y procedimientos a seguir, análisis de vulnerabilidades y planes de contingencia.

Entrevistado 2: Como políticas de Protección, software para monitorear la información personal, seguridad y monitoreo.

Pregunta 6

¿Cuáles son las principales vulnerabilidades y desafíos que enfrenta el estado en la protección de los datos personales frente a los avances tecnológicos?

Entrevistado 1: Las claves inseguras en sistemas informáticos de la UEB y correos electrónicos.

Entrevistado 2: Software mal intencionado, un hacker que trate de robar información personal.

Pregunta 7

¿Cómo afecta la falta de concienciación ciudadana sobre la protección de los datos personales a la eficacia de la legislación ecuatoriana en esta materia?

Entrevistado 1: Afecta gravemente, más por el desconocimiento y no se dimensionan las consecuencias.

Entrevistado 2: Mal intencional la información que hay en instituciones públicas, beneficiarse de información personal y hacer mal uso de la misma.

Pregunta 8

¿Qué recomendaciones pueden hacerse para mejorar la legislación y los mecanismos de protección de datos personales frente a las nuevas amenazas digitales?

Entrevistado 1: Generar políticas internas rígidas de seguridad. Detallar los procedimientos a seguir en caso de detección de vulnerabilidades.

Entrevistado 2: Capacitación al personal de tecnología, monitoreo constante, implementar mecanismos o software que maneje los datos, también la realización de auditorías constantes.

4.2.Encuestas

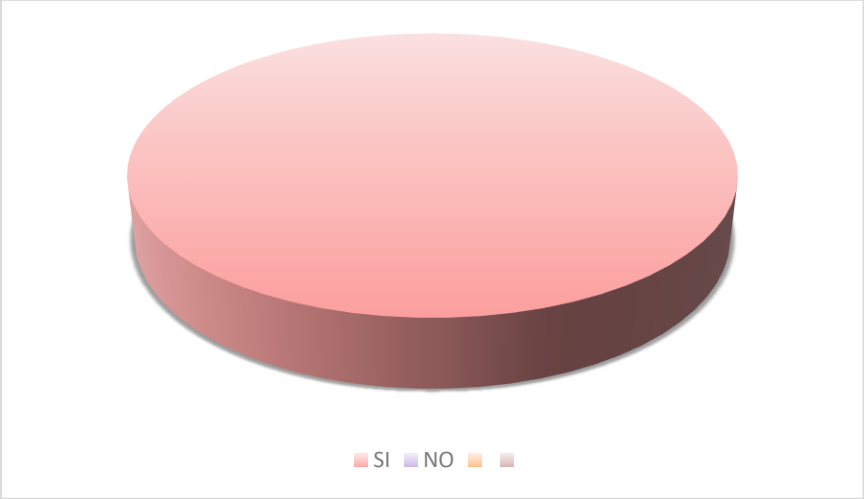
PREGUNTA 1

¿Considera que la Constitución de la República del Ecuador garantiza de manera adecuada el derecho a la protección de datos personales?

Tabla No. 1

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

Gráfico No. 1



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados considera que la Constitución de la República del Ecuador garantiza de manera adecuada el derecho a la protección de datos personales. La totalidad de ciudadanos encuestados coincidían en qu nuestra Constitución tiene exceso de derechos

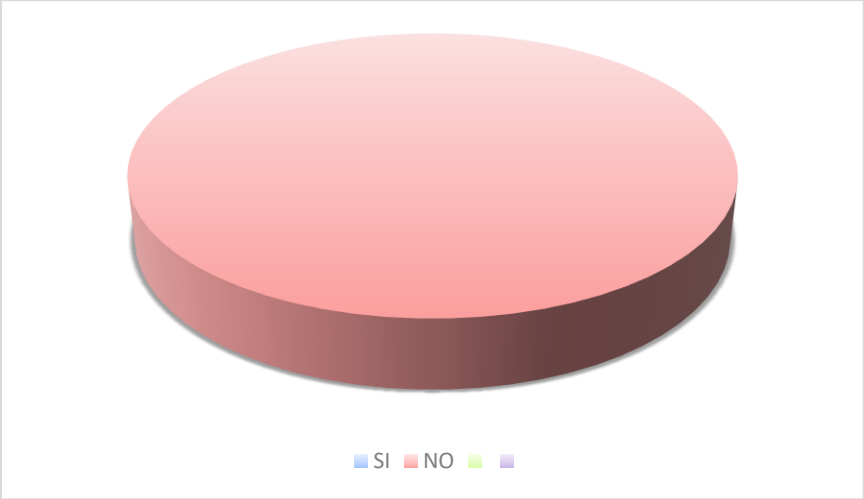
PREGUNTA 2

¿Cree que el Código Orgánico Integral Penal establece sanciones suficientes para el uso indebido de datos personales?

Tabla No. 2

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

Gráfico No. 2



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados cree que el Código Orgánico Integral Penal no establece sanciones suficientes para el uso indebido de datos personales. La inseguridad que sienten los ciudadanos sobre la falta de protección legal de sus datos es determinante en esta pregunta, pues no hay sanciones fuertes para el mal manejo de datos personales.

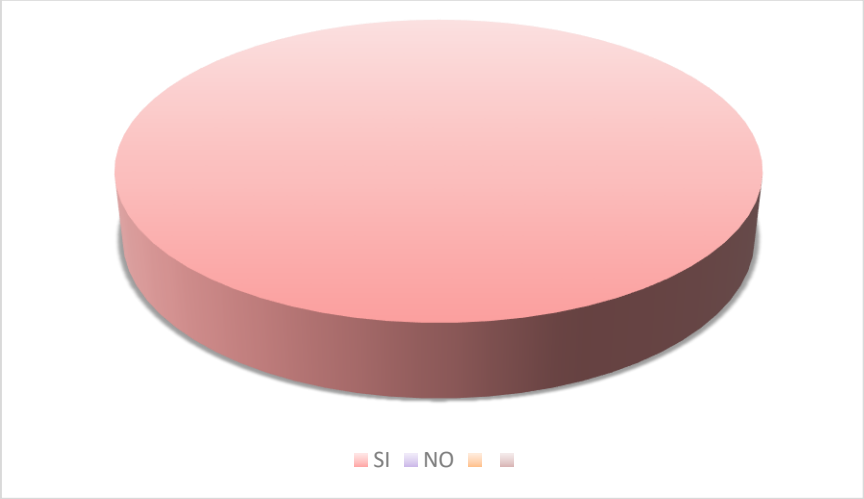
PREGUNTA 3

¿Piensa que la Ley Orgánica de Protección de Datos Personales, aprobada en 2021, es efectiva para regular el tratamiento de los datos personales en el ámbito tecnológico?

Tabla No. 3

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

Gráfico No. 3



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados piensa que la Ley Orgánica de Protección de Datos Personales, aprobada en 2021, no es efectiva para regular el tratamiento de los datos personales en el ámbito tecnológico. Esta respuesta actualmente en el año 2024, demuestra que aún no se sienten efectos positivos de la promulgación de esta normativa.

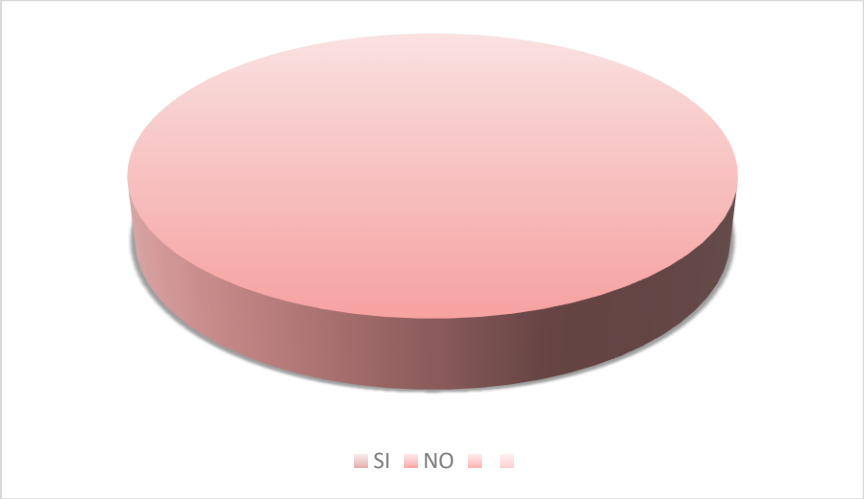
PREGUNTA 4

¿Está usted de acuerdo en que las empresas tecnológicas que operan en el Ecuador cumplen con las normativas de protección de datos personales vigentes?

Tabla No. 4

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

Gráfico No. 4



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados está de acuerdo en que las empresas tecnológicas que operan en el Ecuador no cumplen con las normativas de protección de datos personales vigentes. Esta pregunta refuerza los resultados obtenidos en anteriores preguntas, puesto que, los ciudadanos sienten que no existe protección de datos personales por parte de las empresas tecnológicas en nuestro país.

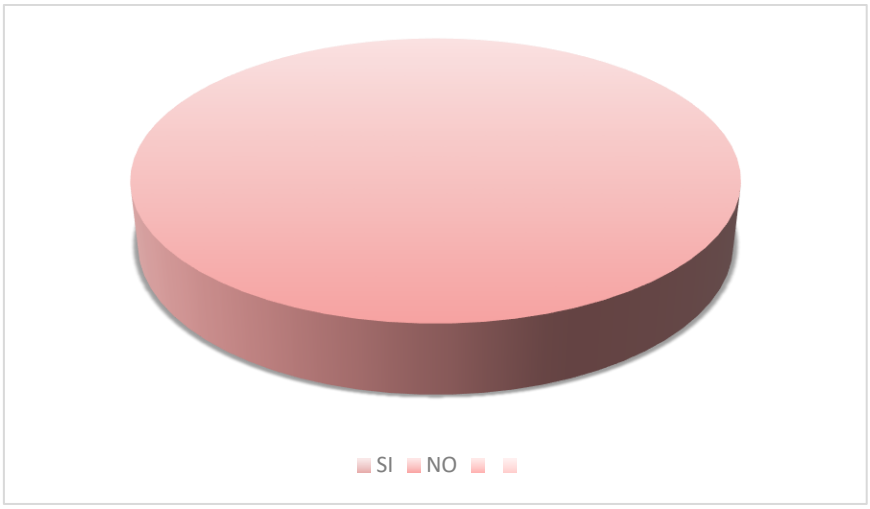
PREGUNTA 5

¿Considera que el Ecuador cuenta con un mecanismo adecuado para que las personas puedan ejercer sus derechos relacionados con la protección de sus datos personales?

Tabla No. 5

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

Gráfico No. 5



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados considera que el Ecuador no cuenta con un mecanismo adecuado para que las personas puedan ejercer sus derechos relacionados con la protección de sus datos personales. Sale a relucir el desconocimiento del contenido de la Ley Orgánica de Protección de Datos por parte de la ciudadanía, lo que se muy preocupante.

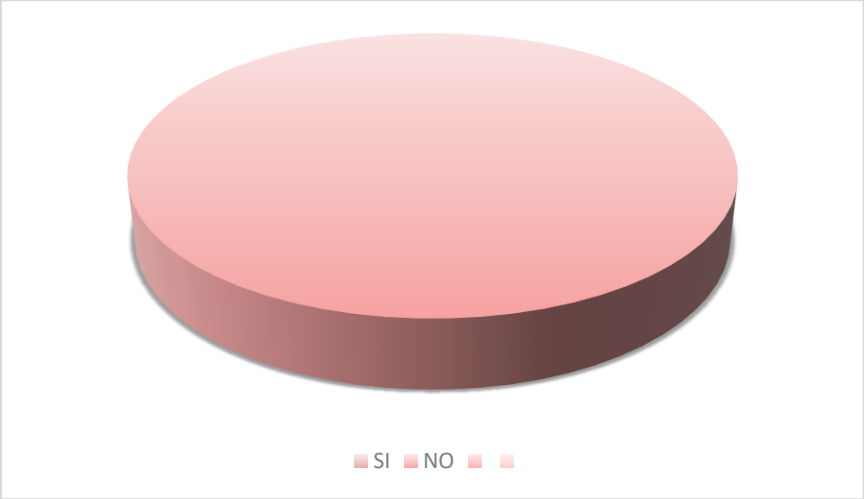
PREGUNTA 6

¿Cree que la Superintendencia de Protección de Datos Personales, creada por la ley, tiene los recursos y capacidades suficientes para desempeñar su rol?

Tabla No. 6

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

Gráfico No. 6



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados cree que la Superintendencia de Protección de Datos Personales, creada por la ley, no tiene los recursos y capacidades suficientes para desempeñar su rol. Esta respuesta es lógica por cuanto apenas esta creada y se encuentra en proceso de estructuración.

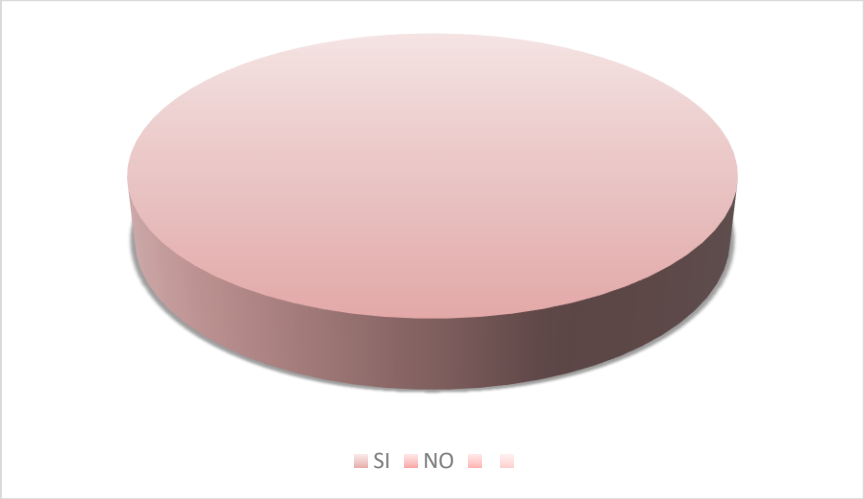
PREGUNTA 7

¿Está de acuerdo en que las herramientas tecnológicas disponibles en el Ecuador son seguras para proteger los datos personales de los usuarios?

Tabla No. 7

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

Gráfico No. 7



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los ciudadanos encuestados está de acuerdo en que las herramientas tecnológicas disponibles en el Ecuador no son seguras para proteger los datos personales de los usuarios. La ciudadanía siente inseguridad con respecto a la protección de sus datos personales, esto está latente.

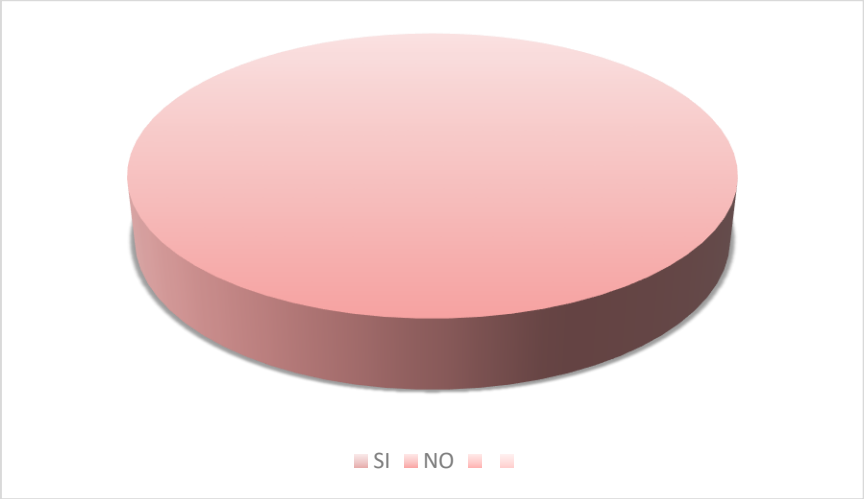
PREGUNTA 8

¿Piensa que los ciudadanos conocen y entienden plenamente sus derechos sobre la protección de sus datos personales?

Tabla No. 8

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

Gráfico No. 8



Investigador: *Melany Iveth Garcés Llanos.*

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

ANÁLISIS: El cien por ciento de los piensa que los ciudadanos no conocen y entienden plenamente sus derechos sobre la protección de sus datos personales. El desconocimiento de la novísima normativa es evidente, lo que podría traducirse como una falta de socialización de los organismos del estado para fomentar su aplicación y conocimiento.

4.3.Discusión

La investigación sobre los mecanismos jurídicos establecidos en la legislación ecuatoriana para proteger los datos personales en la era de las tecnologías de la información resalta la relevancia y los desafíos de garantizar la privacidad y la seguridad en un entorno digital cada vez más complejo. La Ley Orgánica de Protección de Datos Personales, promulgada en 2021, representa un avance significativo en el marco normativo del país, alineándose con estándares internacionales como el Reglamento General de Protección de Datos (GDPR). Sin embargo, su implementación práctica plantea retos que requieren atención estatal e implantación de políticas públicas que permitan efectivizar el derecho a la protección de datos personales en nuestro país.

La Ley Orgánica de Protección de Datos Personales establece principios claros como la licitud, transparencia, minimización de datos y responsabilidad proactiva, que guían el tratamiento de los datos personales. La creación de la Superintendencia de Protección de Datos Personales es un avance crucial, pues centraliza la supervisión y refuerza la capacidad del Estado para garantizar el cumplimiento de la normativa.

Adicionalmente, los derechos otorgados a los titulares de datos, como el acceso, rectificación, supresión y portabilidad, empoderan a los ciudadanos y promueven un control efectivo sobre su información; estos mecanismos son esenciales para mitigar los riesgos asociados al tratamiento masivo de datos en sectores como la salud, la educación y el comercio electrónico.

En la era digital, tecnologías como el big data, la inteligencia artificial y el internet de las cosas han multiplicado la capacidad de las entidades públicas y privadas para recopilar, analizar y utilizar datos personales; esto aumenta el riesgo de vulneraciones a la privacidad, como el uso indebido de datos o las filtraciones masivas. En este contexto, la

Ley Orgánica de Protección de Datos Personales enfrenta el desafío de regular un entorno en constante evolución, donde las tecnologías emergentes pueden superar las capacidades regulatorias tradicionales.

La protección de datos personales como un derecho fundamental autónomo representa un avance crucial en la garantía de los derechos humanos en la era digital; su reconocimiento y desarrollo en sistemas jurídicos como el ecuatoriano reflejan la necesidad de responder a los desafíos de la sociedad interconectada. Sin embargo, para que esta autonomía sea efectiva, es necesario fortalecer los mecanismos regulatorios y promover una mayor conciencia ciudadana sobre su importancia. En última instancia, este derecho autónomo es esencial no solo para proteger la privacidad, sino también para garantizar la dignidad y libertad de las personas en un mundo cada vez más digitalizado.

La regulación de las transferencias internacionales de datos también es un tema crítico. Si bien la Ley Orgánica de Protección de Datos Personales establece condiciones para garantizar un nivel adecuado de protección en el extranjero, la globalización de los flujos de datos plantea interrogantes sobre la efectividad de estas disposiciones en la práctica.

Aunque la norma proporciona mecanismos para la protección de datos, su implementación efectiva enfrenta varios obstáculos: Muchas personas desconocen sus derechos como titulares de datos y los mecanismos disponibles para protegerlos. Esto limita el ejercicio pleno de las garantías previstas en la ley; La Superintendencia de Protección de Datos requiere recursos humanos, técnicos y financieros suficientes para cumplir con su mandato. Sin una supervisión efectiva, la normativa corre el riesgo de convertirse en una herramienta inoperante. Además, la adaptación a las exigencias legales, como la realización de evaluaciones de impacto o el mantenimiento de registros de

actividades de tratamiento, representa un reto considerable, especialmente para las pequeñas y medianas empresas; ya que, tecnologías como la inteligencia artificial y el análisis de datos masivos pueden hacer que el tratamiento de datos sea opaco, dificultando el cumplimiento de principios como la transparencia y la proporcionalidad.

Al comparar la Ley Orgánica de Protección de Datos Personales con el Reglamento General de Protección de Datos (GDPR), se observan similitudes significativas, como la adopción de derechos para los titulares y la inclusión de principios rectores en el tratamiento de datos. Sin embargo, el estado ecuatoriano enfrenta desafíos específicos relacionados con su capacidad institucional y la madurez de su cultura de protección de datos.

Por ejemplo, mientras que el GDPR cuenta con un amplio historial de aplicación y una infraestructura regulatoria consolidada en Europa, Ecuador se encuentra en una etapa inicial de implementación; esto subraya la necesidad de fortalecer las capacidades locales y fomentar una cultura de cumplimiento.

La efectividad de la Ley Orgánica de Protección de Datos Personales dependerá en gran medida de cómo se aborden los desafíos mencionados. Es necesario: Incrementar la formación y sensibilización sobre la protección de datos en todos los sectores; fortalecer la cooperación internacional para enfrentar los riesgos transfronterizos; invertir en tecnologías que permitan una supervisión efectiva, como herramientas de auditoría automatizada; y, promover alianzas entre el sector público y privado para garantizar una implementación uniforme de la normativa.

El marco jurídico ecuatoriano establecido por la Ley Orgánica de Protección de Datos Personales es un paso fundamental hacia la protección de los datos personales en la era digital; sin embargo, para que esta ley cumpla su propósito, es esencial superar los

desafíos de implementación y adaptar continuamente la normativa a los avances tecnológicos. Esto requerirá un esfuerzo conjunto de las autoridades, las empresas y la sociedad civil para construir un entorno digital más seguro y equitativo.

CAPÍTILO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Se concluye que el marco legal ecuatoriano, encabezado por la Ley Orgánica de Protección de Datos Personales (LOPDP), establece un sistema normativo que incorpora principios fundamentales, como la licitud, transparencia y proporcionalidad, y derechos para los titulares de datos personales. Aunque esta legislación se alinea con estándares internacionales como el Reglamento General de Protección de Datos (GDPR), su efectividad depende de una implementación adecuada y de la consolidación de la Superintendencia de Protección de Datos Personales como entidad reguladora independiente y eficaz.

El uso, almacenamiento y tratamiento de datos personales en el entorno digital expone a los individuos a riesgos significativos, como la pérdida de privacidad, la discriminación por el uso indebido de datos sensibles y la vulneración de información debido a brechas de seguridad. Estos riesgos se ven exacerbados por el rápido avance de tecnologías como la inteligencia artificial, el big data y el internet de las cosas, que plantean desafíos adicionales para garantizar el cumplimiento de los derechos de los titulares.

Aunque la Ley Orgánica de Protección de Datos Personales establece una base normativa para la protección de datos personales, su efectividad en la preservación de la privacidad y el control de los individuos sobre sus datos personales está limitada por factores como la falta de recursos técnicos y humanos en la autoridad de control, la baja sensibilización de los ciudadanos sobre sus derechos y las asimetrías tecnológicas entre los titulares de datos y las entidades responsables de su tratamiento; superar estas limitaciones

es fundamental para garantizar que las regulaciones sean efectivas y cumplan con su objetivo de proteger los derechos fundamentales en la era digital.

5.2. Recomendaciones

Se recomienda al Gobierno Nacional el fortalecimiento institucional de la Superintendencia de Protección de Datos Personales; es necesario dotar a este organismo de recursos financieros, técnicos y humanos suficientes para cumplir su función de supervisión y regulación; incluyendo la implementación de tecnologías avanzadas para monitorear el cumplimiento de la ley, la realización de auditorías y la capacitación continua del personal.

A La Superintendencia de Protección de datos se recomienda la promoción de la educación y sensibilización sobre la protección de datos personales; desarrollando campañas educativas dirigidas a ciudadanos, empresas y entidades públicas para fomentar la conciencia sobre los derechos relacionados con la protección de datos y las responsabilidades legales; incluyendo talleres, guías prácticas y recursos digitales accesibles para todas las partes interesadas.

A la Asamblea Nacional se recomienda la adaptación constante del marco normativo a las tecnologías emergentes; puesto que es fundamental actualizar periódicamente la legislación y las directrices regulatorias para abordar los riesgos asociados a tecnologías emergentes como la inteligencia artificial, el big data y la blockchain; esto debe incluir la incorporación de nuevas disposiciones que promuevan la transparencia en el uso de estas tecnologías y establezcan medidas específicas para mitigar los riesgos asociados al tratamiento automatizado de datos personales.

BIBLIOGRAFÍA

Bygrave, L. A. (2014). Ley de privacidad de datos: Una perspectiva internacional. Oxford University Press.

Castells, M. (2020). La era de la información: Economía, sociedad y cultura. Fondo de Cultura Económica.

ESET. (2021). Ciberataques en América Latina aumentan un 24% en 2021. ESET Latinoamérica. https://www.eset.com/latam/ciberataques2021

Ferreres Comella, V. (2016). "El derecho fundamental a la protección de datos personales". Revista Española de Derecho Constitucional, 106(2), 9-34.

González Fuster, G. (2014). La emergencia de la protección de datos personales como un derecho fundamental de la UE. Springer.

González, J. (2019). Impacto de la inteligencia artificial en la sociedad. Universidad Autónoma de México.

González, J. (2021). El derecho a la privacidad en la era digital: Un análisis desde la inteligencia artificial y el big data. Revista Jurídica de Protección de Datos, 12(3), 45-60.

González, J. (2021). El principio de licitud en el tratamiento de datos personales: Análisis desde una perspectiva latinoamericana. Revista Jurídica de Protección de Datos, 15(2), 45-67.

González, J. (2021). Impacto de las nuevas tecnologías en la privacidad: Desafíos para la legislación ecuatoriana. Universidad Central del Ecuador.

González, J. (2021). Transparencia y protección de datos en América Latina: Un análisis comparativo entre Argentina y México. Revista de Derecho Comparado, 12(3), 45-60.

Gómez, P. (2019). Privacidad y protección de datos personales en la era digital. Editorial Jurídica Latinoamericana.

Gómez, P. (2020). Protección de datos personales en el Ecuador: Análisis y retos. Revista Jurídica Latinoamericana, 10(2), 45-67.

Gómez, P. (2021). Privacidad y protección de datos personales en América Latina: Desafíos en la era digital. Editorial Jurídica Latinoamericana.

Gómez, P. (2021). Protección de datos personales en América Latina: Desafíos y perspectivas en la era digital. Editorial Jurídica Latinoamericana.

Gutiérrez, A. (2020). Protección de datos personales en la era digital: Análisis comparativo de las normativas europeas y latinoamericanas. Quito: Editorial Jurídica.

Maldonado, F. (2020). El consentimiento en el tratamiento de datos personales en México: Un análisis comparativo con el GDPR. Revista de Derecho Comparado, 8(1), 32-51.

Maldonado, F. (2020). El principio de transparencia en el tratamiento de datos personales: Un análisis de las políticas de privacidad en el entorno digital. Revista Latinoamericana de Derecho, 8(2), 34-52.

Maldonado, F. (2020). La era digital y los retos para la privacidad: Un análisis desde América Latina. Revista de Ciencias Sociales, 15(3), 60-75.

Maldonado, F. (2021). La digitalización en América Latina: Retos y oportunidades. Revista Latinoamericana de Tecnología.

Mendez, A. (2020). La protección de datos personales en América Latina: Retos y avances. Revista Jurídica Latinoamericana, 45(2), 123-145.

Mendoza, L. (2020). Ética en la era del big data: Desafíos para la privacidad. Revista de Ciencias Sociales, 12(3), 45-59.

Mendoza, L. (2020). Intimidad y privacidad en el contexto digital: Desafíos para la legislación latinoamericana. Universidad Autónoma de México.

Mendoza, L. (2020). La ética en la era del big data: Implicaciones para la protección de datos personales. Revista de Ciencias Sociales, 15(3), 60-75.

Mendoza, L. (2020). La era digital y los retos para la protección de datos personales en América Latina. Revista de Ciencias Sociales, 15(3), 60-75.

Mora, S. (2021). La nueva Ley Orgánica de Protección de Datos Personales en Ecuador: Desafíos y oportunidades. Guayaquil: Ediciones Derecho Digital.

Naciones Unidas. (1948). Declaración Universal de los Derechos Humanos.

Naciones Unidas. (1966). Pacto Internacional de Derechos Civiles y Políticos

Organización de los Estados Americanos (OEA). (1969). Convención Americana sobre Derechos Humanos.

Parlamento Europeo. (2016). Reglamento General de Protección de Datos (Reglamento UE 2016/679).

Pereira, A. & Sánchez, R. (2022). "Protección de datos en América Latina: desafíos y avances." Revista Derecho y Tecnología, 14(2), 45-67.

Ramírez, J., & Torres, M. (2022). El desafío de la protección de datos en la era digital en Ecuador. Revista de Derecho y Tecnología, 12(1), 85-97.

Romero, A. (2021). La Ley Orgánica de Protección de Datos Personales en Ecuador: Un análisis comparativo con el GDPR. Revista de Derecho Comparado, 8(1), 32-51.

Romero, A. (2021). La Ley Orgánica de Protección de Datos Personales en Ecuador: Un análisis desde el principio de transparencia. Universidad de Cuenca.

Romero, A. (2021). La protección de datos personales en Ecuador: Una mirada crítica. Universidad de Cuenca.

Superintendencia de Protección de Datos Personales del Ecuador. (2022). Informe Anual de Actividades. Quito.

Lexigrafía

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

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial, 460.