UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE DERECHO

Tema: Análisis de la actual legislación ecuatoriana sobre la protección de datos personales en el entorno digital: Evaluación de su eficacia y desafíos.

Trabajo de titulación previo a la obtención del
Título de Abogado

AUTOR: Diego Stalyn Yucailla Caiza
TUTOR: Abg. Cristian Gabriel Borja Tipán, Mgtr.

Quito-Ecuador
2025

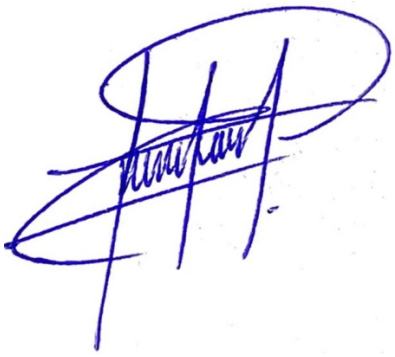
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Diego Stalyn Yucailla Caiza con documento de identificación N° 1722054887 manifiesto que:

Soy el autor y responsable del presente trabajo, declaro que he utilizado herramientas de inteligencia artificial solo para fines de investigación, lo cual consta en la citas y referencias; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 7 de febrero del año 2025

Atentamente,



Yucailla Caiza Diego Stalyn
1722054887

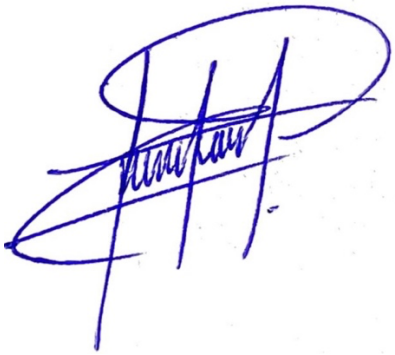
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Diego Stalyn Yucailla Caiza con documento de identificación No. 1722054887, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: Análisis de la actual legislación ecuatoriana sobre la protección de datos personales en el entorno digital: Evaluación de su eficacia y desafíos, el cual ha sido desarrollado para optar por el título de: Abogado, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 11 de febrero del año 2025

Atentamente,



Yucailla Caiza Diego Stalyn
1722054887

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Cristian Gabriel Borja Tipán con documento de identificación N° 1718409871, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE LA ACTUAL LEGISLACIÓN ECUATORIANA SOBRE LA PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO DIGITAL: EVALUACIÓN DE SU EFICACIA Y DESAFÍOS, realizado por Diego Stalyn Yucailla Caiza con documento de identificación N° 1722054887, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 26 de febrero del año 2025

Atentamente,

Cristian Gabriel Borja Tipán
CC 1718409871

Índice de contenido

Resumen

La presente investigación analiza la eficacia del marco jurídico ecuatoriano para la protección de los datos personales de los ciudadanos en el entorno digital, así como los principales problemas y desafíos que lo subyacen. Como resultado, se encontró que, a pesar de la existencia en Ecuador de legislaciones formalmente apropiadas, el marco legal sobre datos personales contiene obstáculos estructurales, institucionales y culturales que impiden su aplicación y la "garantía" de un derecho fundamental a la autodeterminación informativa. Atendiendo al objetivo de la investigación, se trataba de la evaluación de la Ley Orgánica de Protección de Datos Personales con la identificación de las fortalezas y debilidades, así como el nivel de su cumplimiento con los estándares internacionales, en concreto, el Reglamento General de Protección de Datos de la Unión Europea. El enfoque metodológico relativo se basa en los métodos cualitativos y comprende el análisis y la evaluación normativa, así como las entrevistas con expertos académicos en derecho digital y ciberseguridad. Los principales resultados son que, a pesar del progreso dado por la legislación a principios de 2021, existen vacíos importantes en el campo de la regulación penal y la protección de la niñez. Además, existe una cultura insuficiente de la institución de la privacidad, una formación técnica deficiente en las entidades públicas y deficiencias en los mecanismos de control. Los expertos entrevistados han señalado la falta de recursos, formación y herramientas efectivas para garantizar una protección real. Por lo tanto, la legislación ecuatoriana debería fortalecerse en el marco de una perspectiva estructural con referencia al modelo europeo. Es indispensable incorporar medidas como la responsabilidad proactiva, evaluaciones de impacto, una autoridad de control verdaderamente independiente y una estrategia nacional de educación digital.

Palabras clave: Digital, información, protección de datos, seguridad, tecnología

Abstract

This research analyzes the effectiveness of the Ecuadorian legal framework in protecting citizens' personal data in the digital environment, as well as the main underlying problems and challenges. It was found that, despite the formal adequacy of existing legislation in Ecuador, the legal framework on personal data contains structural, institutional, and cultural barriers that hinder its enforcement and the actual guarantee of the fundamental right to informational self-determination. The objective of the study was to evaluate the Organic Law on Personal Data Protection, identifying its strengths and weaknesses, as well as its level of compliance with international standards—specifically, the European Union's General Data Protection Regulation (GDPR). The methodological approach followed a qualitative design, including legal analysis and expert interviews with scholars specializing in digital law and cybersecurity. The main findings reveal that, despite progress brought by the legislation in early 2021, significant gaps remain in areas such as criminal regulation and child protection. Furthermore, there is a weak privacy culture, insufficient technical training in public institutions, and deficiencies in oversight mechanisms. Interviewed experts pointed to a lack of resources, training, and effective tools to ensure real protection. Therefore, Ecuadorian legislation should be strengthened through a structural perspective aligned with the European model. It is essential to incorporate measures such as proactive accountability, impact assessments, a truly independent supervisory authority, and a national strategy for digital education.

Keywords: Digital, information, data protection, security, technology.

1. INTRODUCCIÓN

El entorno digital ha configurado un hábitat complejo donde los seres humanos encuentran nuevos modos de interacción; este entramado de relaciones representa una extensión de la realidad material a la que estamos acostumbrados por naturaleza. Es así que, aparece la era digital a inicios de los años 1990 con el nacimiento de internet generando prestaciones de gran impacto como las derivadas de las tecnologías de información y la comunicación para acelerar la transmisión de los datos y la conexión internacional para fortuna de la comunidad global. En la misma medida de los beneficios, emergen delitos en una gama amplia de tipificaciones exponiendo a un riesgo constante a la comunidad interconectada en estos entornos, convirtiendo a la era digital en una transición necesaria de la vida contemporánea hacia nuevos beneficios y peligros.

Al analizar la utilización de la legislación actual sobre protección de datos personales en el entorno digital, es importante tener en cuenta cómo otros sistemas jurídicos enfrentan este problema. La protección de datos personales tiene algunas definiciones y utilizaciones alrededor del mundo. Históricamente, según Vivar (2022), la protección de datos personales tiene sus inicios como un derecho a la vida privada, se da en los finales del siglo XIX. No obstante, en el siglo XX el derecho a la vida privada tiene una mayor acogida, lo que nos hace referencia en la declaración de las Naciones Unidas sobre los inicios del derecho humano a la vida privada (Arcos, et.al, 2023).

El mundo entero está encaminado hacia nuevas maneras de vida inmersas en tecnología digital; estos avances generan libertades en las que hacen parte de una vida diaria de la que no podemos persuadir. La era digital nos ha permitido optimizar procesos que han representado históricamente la base para el desarrollo como la comunicación, educación, movilidad, etc. Es decir que con el avance tecnológico se han acortado las distancias y hemos podido cruzar fronteras mediante la comunicación. Creando áreas donde se realiza la vida actual del ser humano en el cual requieren la presencia y protección de las instituciones privadas, públicas y el estado para proteger los derechos de las personas, así rebajar los peligros y riesgos que implican.

En el momento actual la mayor parte de los países regulan la protección de datos personales para proteger y garantizar, el derecho a la privacidad y seguridad, para lo cual no se pueda permitir el uso indebido de la misma y las personas puedan tener libre acceso y controlar su

información. También el objetivo de fortalecer el desarrollo de empresas que se encarguen y resguarden la protección de datos personales realizando un aporte significativo, ofrecer la seguridad y confianza que se necesita y por ende el buen manejo de la información digital, por lo que este servicio fomente a la seguridad interna de un país, y así realizar, fomentar políticas que ayuden al desarrollo tecnológico, mejor manejo de la información pública y personal de acuerdo con lo que menciona (Martínez, Plúas, & Muñoz, 2024).

Nuestro país, enfrenta desafíos característicos de sistemas legislativos marcados por vacíos e incoherencias, propios de una institucionalidad débil. Esta realidad se refleja en una sociedad que se ve fragilidades internas relacionadas con la debilidad estatal. Es por esto que resulta relevante contar con un informe actualizado sobre la situación y los retos de la legislación ecuatoriana en lo que a protección de datos personales en el entorno digital se refiere.

De esta manera, Barreto (2023) subraya la necesidad de que el país se convierta en una zona segura para realizar transacciones internacionales, lo que ampliaría la confianza tanto en empresas ecuatorianas como en las extranjeras que invierten en su territorio. Al mismo tiempo, Jurado, Riera & Méndez (2023) sostienen que debe garantizarse la seguridad de las niñas, los niños y adolescentes ecuatorianos, mediante el fortalecimiento del marco constitucional adecuado y la implementación de políticas públicas en la actualidad digital.

El trabajo tiene como objetivo el análisis de la legislación ecuatoriana en una de las áreas más actuales y controvertidas: la protección de datos personales en el entorno digital. Este objetivo implica el análisis de las fortalezas y debilidades y la medida en que se adapta a los estándares internacionales y regionales. Para lograr este objetivo, este trabajo propone el estudio del marco jurídico ecuatoriano y su aplicación con respecto a la esfera digital, la comparación de la legislación ecuatoriana con el Reglamento General de Protección de Datos europeo. El estudio abordará los desafíos iniciales y propondrá recomendaciones.

2. MÉTODO CIENTIFICO

El enfoque cualitativo de esta investigación es exploratorio y descriptivo, el cual se basa en el análisis de documentos y normativas de Ecuador, la región y a nivel global relacionado con la protección de datos personales en la era digital. En este aspecto, se revisarán las leyes, reglamentos y normativa respecto a la materia en Ecuador para presentar y describir el estado

de la legislación en el país, y cuál la actualidad las mayores preocupaciones y logros de la protección de datos personales, incluyendo las limitaciones.

Posteriormente, se procederá a una revisión bibliográfica especializada y a un análisis comparativo con normativas internacionales, dado que no existen bases de datos nacionales referentes a este fenómeno sociopolítico. Mediante esta revisión de literatura se busca contextualizar la problemática desde una perspectiva global, regional y local, lo cual permitirá contar con elementos para comparar el desarrollo legislativo de Ecuador frente a estándares internacionales.

Finalmente, como parte del proceso metodológico, se realizarán entrevistas semi estructuradas a expertos en derecho digital y ciberseguridad. El objetivo de estas entrevistas es contrastar y complementar los hallazgos obtenidos en las fases previas para validar o refutar la hipótesis de estudio.

3. RESULTADOS

3.1 Cronología histórica de la protección de datos personales

El avance tecnológico ha facilitado la propagación masiva de información, lo que incrementa los riesgos y potenciales daños a los derechos de las personas. En este contexto tecnológico y globalizado, se generan nuevos sistemas y procesos automatizados o simples procedimientos capaces de crear perfiles personales a partir de grandes volúmenes de datos, exponiendo a las personas a violaciones de su privacidad y otros derechos esenciales.

El derecho a la protección de los datos personales nace del derecho a la intimidad, aunque con el tiempo ha evolucionado hasta adquirir independencia, reconocida por la jurisprudencia y luego a través de leyes y regulaciones, incluso a nivel constitucional (Argudo, Pinos, & Mora, 2023). En sus inicios se dirigía especialmente hacia la protección de datos íntimos o sensibles, es decir, aquellos que permiten identificar aspectos profundos de una persona, como su ideología, raza, orientación sexual o situación económica.

En una perspectiva posterior, también se incluyeron en la protección legal los datos personales que en realidad podrían no parecer tan susceptibles a la divulgación porque su acumulación y procesamiento podrían llevar a la forma completa de un perfil que puede afectarse la esfera privada de un individuo. De hecho, incluso aunque algunos datos puedan parecer inofensivos

si se toman solos, pueden interpretarse de manera diferente cuando se combinan y ofrecer detalles valiosos inherentes a una persona en particular (Jurado, Riera, & Méndez, 2023). Por lo tanto, todos los datos asociados que posee una persona deben cubrirse con la protección de la ley en la actual redacción.

Por consiguiente, la protección de datos personales no se relaciona de forma directa con la protección de la información en sí, sino con la protección de los derechos de los individuos cuya privacidad pueden verse afectadas. El propósito fundamental es garantizar la autodeterminación informativa, que implica el derecho de cada individuo a decidir cómo se utilizan sus datos personales, independientemente de su naturaleza, no limitándose únicamente a aquellos relacionados con la privacidad o la intimidad, sino abarcando incluso datos que puedan parecer insignificantes. Esto se hace para permitir que cada persona pueda construir su identidad social libremente y evitar las repercusiones negativas que podrían surgir por valoraciones erróneas, no autorizadas o indeseadas sobre su información.

Por ello, es imprescindible establecer altos estándares y garantías en la protección de los datos personales, ya que esta protección no solo resguarda la información, sino que también constituye una herramienta clave para garantizar otros derechos fundamentales. La forma en que se recopila procesa y difunde la información personal incide de manera directa en la libertad individual, especialmente en una sociedad donde lo digital y lo real están cada vez más ligados.

3.2 El reconocimiento del derecho a la protección de datos en Ecuador

La reforma constitucional de 1996 en Ecuador fue un hito relevante al modificar la Constitución de 1976, pues introdujo la garantía jurisdiccional del habeas data (Naranjo Godoy, 2017). La Constitución ecuatoriana de 2008 fue la primera en reconocer explícitamente el derecho a la protección de datos personales, inspirándose en el modelo europeo y buscando alcanzar altos niveles de resguardo en esta materia. El artículo 66, numeral 19, de la Constitución expone claramente que uno de los aspectos principales de este derecho es la autodeterminación informativa (Lucero, 2023). Esto significa que no solo se garantiza el acceso a los datos personales, como ocurría en legislaciones anteriores mediante el hábeas data y las constituciones de 1978 y 1998, sino también que se otorga a los ciudadanos la facultad de decidir sobre la utilización de su información.

Pineda &Quezada (2022) explican que, el surgimiento de este derecho fundamental tiene como base la libertad de autodeterminación informativa, es decir, la facultad individual para controlar todo lo que se refiere a la obtención, gestión, posesión y transmisión de los propios datos personales. Asimismo, se reconoce que los datos personales constituyen el bien protegido y que sólo pueden ser utilizados bajo el principio de legalidad y para los propósitos específicos para los que fueron recabados. De tal manera, la Constitución protege los datos en sí mismos, ya que pueden ser procesados y utilizados para generar perfiles concretos sobre las personas, exponiendo a los titulares a posibles vulneraciones de sus derechos fundamentales consagrados en la constitución.

Sin embargo, Martínez, (2022) señalan que el texto constitucional deja varios aspectos imprecisos, pues no hay una definición precisa de lo que son los datos personales ni se incluyen medidas preventivas o directrices claras sobre su tratamiento, ya sea por parte de organismos públicos o privados, tanto en el ámbito nacional como internacional. De forma similar, Barreto (2023) cuestiona el uso indistinto de los términos “dato” e “información” en la Constitución, argumentando que existe una diferencia significativa: el dato es la unidad mínima que representa hechos, instrucciones o conceptos, mientras que la información surge tras el procesamiento de los datos, etapa en la que adquieren valor y utilidad.

Por lo tanto, la finalidad del derecho a la protección de datos personales es asegurar que las personas tengan control sobre la información que les pertenece. Este derecho no debe confundirse con el derecho a la intimidad o la privacidad, pues su alcance es mucho más amplio. No sólo se protege la información íntima, privada o sensible, sino que todo tipo de dato personal queda amparado, incluso aquellos que parecen insignificantes o sin importancia. Esta protección se justifica porque, según cómo sean tratados, procesados o difundidos, cualquier dato personal tiene el potencial de afectar el libre desarrollo de la personalidad y otros derechos de una persona.

A nivel nacional, el Estado ha impulsado diversas iniciativas como políticas y estrategias orientadas a salvaguardar los datos personales. Cevallos (2021) explica que, la seguridad de la información y la protección de los datos personales como elementos clave para consolidar la sociedad de la información y el conocimiento, así como para fortalecer la confianza de la ciudadanía en el uso de las tecnologías de la información y comunicación. En el mismo sentido, el Plan de la Sociedad de la Información y del Conocimiento 2018-2021 propuso, dentro de su

sexto eje de trabajo dedicado a este tema, tres proyectos dirigidos a garantizar el manejo adecuado de los datos personales tanto en organizaciones públicas como privadas, promoviendo además la corresponsabilidad de la ciudadanía.

Además, el Plan Nacional de Gobierno Electrónico 2018-2021 promovió el establecido en el programa "Gobierno abierto". El usó de una de sus estrategias se destina a la protección de la información y los datos personales. Para cumplir con esta tarea, la prioridad fue dada a la creación de una normativa legal central que se usaría para apoyar la implementación y operación de un sistema integral que proteja este derecho fundamental, El Plan Ecuador Digital 2021, en su componente "Ecuador eficiente y ciberseguro", expresó la gravedad de los temas de ciberseguridad y protección de datos; según se indicó en las garantías necesarias para proteger a la población de las nuevas amenazas digitales y, al mismo tiempo, alentar el desarrollo de la economía digital necesaria para el progreso del país (Carrillo, 2022). En este sentido, se encargó al gobierno del país sudamericano liderar la redacción del Proyecto de Ley Orgánica de Protección de Datos Personales, los cuales se debatieron y aprobaron en la Asamblea Nacional.

3.3 Ley Orgánica de Protección de Datos Personales

El 26 de mayo de 2021 se promulgó la Ley Orgánica de Protección de Datos Personales, que tiene como objetivo la salvaguarda del derecho fundamental de las personas a controlar y proteger su información. La ley persigue al acceso y autodeterminación de sus titulares y establece los principios, deberes y mecanismo de garantía aporte a sujetos de derechos, públicos y privados, asigna la protección de los datos personales también para los ecuatorianos en caso de tratamiento en el extranjero.

En particular, la legislación establece que el consentimiento para manipular estos datos debería ser otorgado de forma libre, específica, informada y sin ambigüedades; esta condición otorga a cada individuo el poder de decidir quién, cómo, cuándo y con qué fin trata su información; además, cualquier tratamiento de datos debe ser realizado con fines legítimos, recogidos y justificados, enmendables por la Autoridad de Protección de Datos Personales.

La legislación vigente incluye dieciséis principios rectores, que han sido incorporados repetidamente no solo en las correspondientes normas internacionales, sino también en la doctrina legal. Así, normas como las Directrices de la OCDE de 1980 sobre la Protección de la

Privacidad y el Flujo Transfronterizo de Datos Personales, la Resolución 45/95 de la Asamblea General de las Naciones Unidas de 1990 y la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas del año 2012, reconocen principios esenciales como la lealtad, transparencia, finalidad, minimización de datos, proporcionalidad, confidencialidad, exactitud y conservación (Lucero, 2023). A su vez, la idea de responsabilidad proactiva ha sido resaltada por enfoques modernos, tales como "Privacy by Design" y la resiliencia cibernética, los cuales exigen mayores estándares de diligencia y anticipación por parte de quienes manejan datos personales.

En el nivel normativo, a los titulares de los datos personales se otorgan derechos específicos con un auténtico grado de protección de conformidad con los artículos adecuados de la legislación. Uno de los derechos fundamentales es conceptualmente el derecho a la información, una responsabilidad de los responsables de informar a los titulares de los datos de manera clara y transparente con respecto a la finalidad de tratamiento, fundamento legal aplicable, el plazo de conservación, la identificación del responsable y administrativo, y las posibles consecuencias del tratamiento.

De igual forma, las normas reconocen los derechos de acceso, rectificación, actualización, supresión de datos y oposición, conforme a los plazos establecidos, por ejemplo, el derecho a recibir respuesta en un plazo de quince días cuando el titular solicite información, correcciones, la eliminación de sus datos o exprese oposición al tratamiento de los mismos en situaciones contrarias a la ley (Ley Orgánica de Protección de Datos Personales, 2021).

Además, la legislación contempla el derecho a no someterse a decisiones fundamentadas única o parcialmente en procesos automatizados, especialmente para proteger contra la realización de perfiles que puedan afectar derechos y libertades fundamentales. Este derecho adquiere especial relevancia para menores de edad, ya que la normativa otorga una protección reforzada a los niños, niñas y adolescentes, respondiendo de esta manera a la necesidad de salvaguardar a los grupos vulnerables (Ley Orgánica de Protección de Datos Personales, 2021). Adicionalmente, la inclusión de un derecho orientado a la educación digital de la ciudadanía busca incentivar el buen uso y la gestión adecuada de las tecnologías de la información, lo que también contribuye a la disminución de las brechas sociales y económicas en el país.

De acuerdo con la misma ley, se define el dato personal como lo que identifica o puede identificar a una persona, ya sea de forma directa o indirecta. Esto implica que la información

protegida puede ser variada en contenido, formato y naturaleza, siempre y cuando permita identificar a su titular, independientemente de si esto requiere o no tecnologías informáticas.

La normativa de protección de datos personales establece una serie de categorías especiales de datos cuyo tratamiento se encuentra estrictamente limitado o prohibido, destacando expresamente los datos sensibles, los relativos a niñas, niños y adolescentes, los datos de salud y aquellos relacionados con personas con discapacidad y sus representantes, en lo referente a información sobre la discapacidad (Cevallos, 2021). Dentro de las disposiciones especiales respecto de los datos sensibles, la ley distingue dos subgrupos: primero, los datos de personas fallecidas, que podrán ser gestionados por cualquier sucesor salvo que el titular haya dispuesto previamente sobre su futuro; y segundo, los datos crediticios, que solo podrán procesarse para fines de evaluación de negocios, conducta comercial o capacidad de pago del titular.

La calificación de un dato como sensible se fundamenta en el posible perjuicio o daño que su divulgación indebida pudiera causar al individuo. Por consiguiente, los datos especialmente protegidos son aquellos cuyo tratamiento poco cuidadoso puede afectar de manera directa la intimidad del individuo y el ejercicio de otros derechos fundamentales,

La normativa establece la opción de comunicar o transferir información personal a terceros siempre que exista un fin legítimo relacionado con las tareas o responsabilidades del encargado o del receptor de dichos datos, y se obtenga previamente la autorización del titular, tal como lo determina el artículo 31 de la Ley. Esta regulación limita la divulgación de datos personales con el objetivo de proteger la privacidad y los derechos del individuo ante posibles usos indebidos (Ley Orgánica de Protección de Datos Personales, 2021). No obstante, la misma ley aclara que no constituirá transferencia o comunicación de información personal cuando exista un contrato específico que establezca claramente los objetivos y condiciones bajo las cuales se realizará el tratamiento de dichos datos.

En materia de seguridad, el marco normativo exige a los responsables y encargados del tratamiento implementar medidas con el objetivo de evitar vulneraciones de derechos. Entre dichas medidas se incluyen la anonimización, seudonimización y la protección de los datos desde el diseño y por defecto, prácticas recogidas también en el Reglamento General de Protección de Datos de la Unión Europea (GDPR, 2016), conforme se refuerza doctrinalmente (Segarra, 2011). Estas disposiciones buscan que quienes gestionan información personal

asuman una responsabilidad activa, garantizando la libertad de elección del titular y su derecho a ser informado previamente, en consonancia con los artículos 23, 27 y 30 de la Ley.

La normativa determina quince obligaciones esenciales que deben observar el responsable y el encargado del tratamiento de datos personales, obligaciones que abarcan desde el uso de medios lícitos, la implementación de procedimientos de evaluación y control de sistemas de seguridad, hasta la formación de políticas de prevención de riesgos. Todo ello pretende una clara asignación de responsabilidades a quienes manejan y tienen acceso a los datos personales, siguiendo la línea del artículo 34 y concordantes.

Asimismo, la ley dispone la designación de un delegado de protección de datos personales en tres supuestos: cuando el tratamiento sea realizado por entidades públicas, cuando se manejen datos personales a gran escala de categorías especialmente protegidas, o cuando la información esté vinculada a la seguridad y defensa nacional (artículo 38). Este delegado queda encargado de funciones de asesoría, control y cooperación con la Autoridad de Protección de Datos Personales, consolidándose como una figura central en el blindaje de los derechos fundamentales vinculados a la protección de datos.

La normativa vigente, alineada con instrumentos internacionales, regula la transferencia internacional de datos personales, permitiendo su flujo únicamente hacia países, organizaciones o entidades que además de ofrecer niveles adecuados de protección, cumplan los estándares internacionales correspondientes. Para asegurar esto, se ha establecido un sistema de control donde la Autoridad de Protección de Datos debe reconocer que el receptor cumple con un sistema de protección adecuado y el encargado del tratamiento debe proporcionar garantías suficientes (Ley Orgánica de Protección de Datos Personales, 2021). De este modo, se acepta la importancia crucial de los flujos transfronterizos de información personal para el comercio y la colaboración en la era digital.

Lo referente al régimen disciplinario, la ley establece rectificaciones a ser tomadas en caso de violación de las normas de protección por parte de controladores y procesadores. Estas medidas incluyen la terminación del procedimiento, la anulación de los datos y la implementación de acciones técnicas, jurídicas o administrativas. Asimismo, la normativa faculta a la Autoridad de Protección de Datos Personales a imponer sanciones económicas, las cuales deben guardar proporcionalidad con la infracción. “Las infracciones leves pueden conllevar multas de uno a diez salarios básicos unificados o el 0,1% al 0,7% del volumen de negocio de la organización

privada, mientras que las graves pueden alcanzar de diez a veinte salarios básicos unificados o el 0,7% al 1% del volumen de negocio" (Cevallos, 2021, p.12).

3.4 La protección de datos personales según el Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos, conocido como RGPD, es una normativa europea que ha transformado la protección de los datos personales en el contexto digital. Entró en vigencia en mayo de 2018, después de ser aprobada en 2016, y su objetivo principal es establecer reglas claras para garantizar la privacidad y la seguridad de la información de las personas que viven en la Unión Europea.

Esta regulación se fundamenta en principios esenciales como la necesidad de obtener el consentimiento claro del titular de los datos, la recopilación de solo aquellos datos estrictamente necesarios, la exactitud de la información, la limitación en el uso de los datos a los fines para los que fueron obtenidos y la protección adecuada para evitar accesos indebidos o alteraciones (Guerrero, 2020). Estos principios son fundamentales para que cualquier proceso de administración de datos personales se lleve a cabo de forma segura y transparente.

Asimismo, el RGPD proporciona a las personas europeas derechos únicos en relación con sus datos personales: acceso a la información que se conserva, corrección de información incorrecta, eliminación y transferencia de datos a otra organización, y negativa a algunos casos de uso de su información. De este modo, se refuerza el control que cada persona tiene sobre sus propios datos.

El Reglamento General de Protección de Datos (2016) reconoce diversos derechos vinculados a la protección de los datos personales, cada uno respaldado por artículos específicos. El artículo 5 establece los principios fundamentales que rigen todo tratamiento de datos personales, tales como la licitud, lealtad, transparencia, finalidad limitada, minimización, exactitud, conservación restringida, integridad, confidencialidad y la responsabilidad proactiva del responsable del tratamiento. Estos principios constituyen el eje normativo que asegura que el tratamiento de los datos personales respete la dignidad y los derechos de las personas físicas.

El derecho de acceso está consagrado en el artículo 15. Este derecho permite a toda persona saber si sus datos personales están siendo tratados, conocer la finalidad de ese tratamiento, las categorías de datos afectadas, los destinatarios o las transferencias previstas, el plazo de

conservación y la existencia de decisiones automatizadas, incluida la elaboración de perfiles (Reglamento General de Protección de Datos, 2016). Esta prerrogativa tiene una función instrumental en el ejercicio de los demás derechos, pues garantiza transparencia y control frente al tratamiento de la información personal por parte de terceros.

La facultad del territorio común de corregir datos erróneos se encuentra en el artículo 16 de RCPD, que reconoce el derecho de rectificación. Este derecho autoriza al propietario para solicitar que el controlador corrija rápidamente los datos defectuosos o lo complete (Reglamento General de Protección de Datos, 2016). La capacidad de garantizar la actualización y autenticidad de la información personal en las bases de datos públicas o privadas es crucial para impedir el perjuicio o la discriminación basada en el uso de registros desactualizados o incorrectos, por lo que es un derecho para salvaguardar la identidad y reputación personales.

El artículo 17 consagra el derecho de supresión, también entendido como derecho al olvido. En ese sentido, el titular de los datos tiene derecho a solicitar la supresión de los datos personales, una vez sus finalidades hayan dejado de ser pertinentes para lo cual fueron recabados, haya retirado su consentimiento, se oponga a su tratamiento, o este sea ilícito (Reglamento General de Protección de Datos, 2016). Este derecho adquiere particular relevancia en el contexto digital, donde la permanencia a perpetuidad de la información puede vulnerar desproporcionadamente la intimidad y dignidad de las personas.

El RGPD también da lugar al derecho a la portabilidad de los datos, según el artículo 20. Este punto permite a los individuos recibir copias de sus datos personales en un formato ordenado, de uso común y entendible por máquina que les permita reutilizar sus datos entre proveedores de servicios (Reglamento General de Protección de Datos, 2016). Su presencia fomenta la autodeterminación informacional y la capacidad de elegir entre plataformas, dado que es posible gestionar la eliminación voluntaria de servicios o sistemas sin la incertidumbre de pérdida de información o la duplicación del proceso de captación.

Según lo establecido en el artículo 21 del reglamento, el titular tiene derecho a oponerse al uso de sus datos personales cuando existan razones específicas vinculadas con su situación particular, particularmente si dicho tratamiento se apoya en el interés legítimo de quien maneja la información o se emplea para fines comerciales o publicitarios. Esta previsión normativa, sumada al artículo 22 que protege el derecho a no quedar sometido únicamente a decisiones

derivadas de procesos automatizados, fortalece la protección del individuo frente a posibles amenazas derivadas de la gestión despersonalizada de sus datos personales en el contexto digital (Reglamento General de Protección de Datos, 2016).

A pesar de ser una ley europea, su influencia se extiende a nivel mundial, ya que cualquier empresa u organización que maneje datos de personas que residen en la Unión Europea está obligada a cumplir con estos requerimientos, sin importar dónde esté situada (Segarra, 2011). Esto ha provocado que muchas entidades de diferentes países adapten sus políticas y prácticas de privacidad para alinearse con los estándares del RGPD.

El RGPD es una normativa relevante en lo que respecta a la privacidad y protección de los datos personales. Es fundamental estar informados sobre los derechos que garantiza y, en el caso de las organizaciones, adoptar las medidas necesarias para proteger los datos de los usuarios conforme a sus disposiciones.

3.5 Desafíos persistentes en la protección de datos

Aunque estas regulaciones están vigentes, el constante desarrollo de las tecnologías digitales y su difusión masiva han favorecido la ocurrencia de infracciones y delitos en materia de privacidad y protección de datos. Entre los delitos que se presentan con mayor frecuencia destacan el acoso, amenazas, vulneración de secretos, agresiones sexuales, coacciones, violencia de género y fraudes. En este sentido, Barreto (2023) indica que las personas cuyos datos son tratados afrontan amenazas significativas, incluyendo suplantación de identidad, extorsión, estafas informáticas, ciberacoso y persecución política.

Los delincuentes cibernéticos emplean los datos personales para afectar la integridad física, psicológica o moral de las personas, o para violentar otros derechos fundamentales. Entre los actos más frecuentes se cuentan el sexting, que implica el envío voluntario de material íntimo que, al ser difundido sin consentimiento, puede vulnerar el derecho a la vida privada. Aunque en Ecuador no existe un tipo penal específico para el sexting, este puede ser sancionado bajo el artículo 178 del Código Orgánico Integral Penal (2014), que trata la violación a la intimidad; el artículo 154, sobre intimidación; y el artículo 103, relativo a pornografía con niñas, niños y adolescentes.

Por otro lado, el grooming implica que un adulto contacte a un menor de edad con fines sexuales, accediendo primero a preferencias o datos personales y luego a material sexual que

utiliza para coaccionar. Esta conducta está tipificada y sancionada en el artículo 173 del COIP, relativo al contacto con finalidad sexual con menores mediante medios electrónicos (Heredia, 2022). El ciberacoso, entendido como amenazas o hostigamiento a través de tecnologías de la información usando datos personales, no cuenta en Ecuador con una figura penal autónoma, pero se incluye dentro del delito de acoso sexual de acuerdo con el artículo 166 del COIP.

La normativa penal ecuatoriana no tipifica de manera precisa la mayoría de delitos informáticos, sino que los sanciona englobándolos en figuras delictivas generales como la estafa o la apropiación fraudulenta por medios electrónicos. Sin embargo, entre 2019 y 2021, la Asamblea Nacional debatió reformas para abordar estas problemáticas en el marco del Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal, con el objetivo de prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2024). La objeción parcial de este proyecto se publicó el 10 de junio de 2021.

3.6 Opinión de expertos

Entrevista No. 1	**Dra. Carolina Andrade Ledesma:** Especialista en Derecho Constitucional
¿Cuál considera que es la principal debilidad jurídica que enfrenta Ecuador en materia de protección de datos personales en el contexto digital?	La falta de una cultura jurídica que comprenda la protección de datos como un derecho humano autónomo, tal como lo reconoce el bloque de constitucionalidad.
¿Qué papel ha jugado la Ley Orgánica de Protección de Datos Personales en el fortalecimiento institucional del país respecto a la seguridad digital?	La Ley Orgánica de Protección de Datos Personales representa un avance formal, pero aún carece de desarrollo jurisprudencial que la conecte con las garantías constitucionales.
¿Cómo evalúa el nivel de preparación de las entidades públicas y privadas en el cumplimiento efectivo de la normativa vigente sobre protección de datos?	Las entidades públicas tienen un desconocimiento generalizado del principio de autodeterminación informativa y pocas cuentan con delegados de protección de datos.

¿Qué rol debería jugar la academia y la investigación jurídica en el diseño de futuras políticas públicas sobre seguridad digital y protección de datos en Ecuador?	La academia debe generar litigios estratégicos y análisis doctrinarios que fortalezcan la aplicación de este derecho desde una visión garantista.

Entrevista No. 2	**Dr. Esteban Muñoz Villacís:** Especialista en delitos informáticos
¿Cuál considera que es la principal debilidad jurídica que enfrenta Ecuador en materia de protección de datos personales en el contexto digital?	Existe una carencia de tipos penales claros para conductas como la suplantación de identidad digital y el uso no consentido de datos sensibles.
¿Qué papel ha jugado la Ley Orgánica de Protección de Datos Personales en el fortalecimiento institucional del país respecto a la seguridad digital?	Aunque la ley tipifica algunas conductas, no hay una articulación eficaz con el Código Orgánico Integral Penal ni capacitación suficiente de fiscales y jueces.
¿Cómo evalúa el nivel de preparación de las entidades públicas y privadas en el cumplimiento efectivo de la normativa vigente sobre protección de datos?	El nivel es deficiente, y muchas instituciones ni siquiera identifican las amenazas más básicas como el phishing o el malware orientado al robo de datos.
¿Qué rol debería jugar la academia y la investigación jurídica en el diseño de futuras políticas públicas sobre seguridad digital y protección de datos en Ecuador?	La investigación jurídica debe vincularse más con la criminología digital y ofrecer propuestas normativas claras para actualizar el COIP.

Entrevista No. 3	**Abg. Paulina Ríos Cedeño:** Asesora jurídica del Ministerio de Gobierno
¿Cuál considera que es la principal debilidad jurídica que enfrenta Ecuador en materia de protección de datos personales en el contexto digital?	La debilidad más notoria es la ausencia de un ecosistema digital robusto que facilite la interoperabilidad segura entre instituciones.

¿Qué papel ha jugado la Ley Orgánica de Protección de Datos Personales en el fortalecimiento institucional del país respecto a la seguridad digital?	La ley ha generado obligaciones formales, pero la falta de presupuesto y recursos humanos limita su implementación real en el sector público.
¿Cómo evalúa el nivel de preparación de las entidades públicas y privadas en el cumplimiento efectivo de la normativa vigente sobre protección de datos?	Muchas instituciones ni siquiera han desarrollado su registro de actividades de tratamiento ni tienen políticas internas actualizadas.
¿Qué rol debería jugar la academia y la investigación jurídica en el diseño de futuras políticas públicas sobre seguridad digital y protección de datos en Ecuador?	Desde la academia se debe trabajar con universidades e institutos públicos para capacitar a los servidores y generar estándares técnicos apropiados.

Entrevista No. 4	**Dr. Marcelo Aguirre Román:** Especialista de delitos informáticos
¿Cuál considera que es la principal debilidad jurídica que enfrenta Ecuador en materia de protección de datos personales en el contexto digital?	La norma ecuatoriana adolece de vaguedad conceptual y no armoniza adecuadamente con estándares internacionales como los del RGPD
¿Qué papel ha jugado la Ley Orgánica de Protección de Datos Personales en el fortalecimiento institucional del país respecto a la seguridad digital?	Ha sido un avance en la transposición de estándares internacionales, pero no existe un sistema sancionador o de supervisión realmente funcional.
¿Cómo evalúa el nivel de preparación de las entidades públicas y privadas en el cumplimiento efectivo de la normativa vigente sobre protección de datos?	El cumplimiento es desigual. El sector financiero y telecomunicaciones tienen más avances, mientras que otros sectores ni siquiera reconocen sus obligaciones.
¿Qué rol debería jugar la academia y la investigación jurídica en el diseño de futuras políticas públicas sobre seguridad digital y protección de datos en Ecuador?	La investigación jurídica debe ser comparativa y propositiva, generando bases doctrinarias que nutran las reformas legislativas en el futuro.

Entrevista No. 5	**Dra. Verónica Tapia Molina:** Jueza de la Unidad judicial de Familia, mujer niñez y adolescencia
¿Cuál considera que es la principal debilidad jurídica que enfrenta Ecuador en materia de protección de datos personales en el contexto digital?	El gran vacío es la falta de protección reforzada a niños, niñas y adolescentes como sujetos hiper vulnerables en entornos digitales.
¿Qué papel ha jugado la Ley Orgánica de Protección de Datos Personales en el fortalecimiento institucional del país respecto a la seguridad digital?	La ley apenas hace referencias generales a grupos de atención prioritaria, sin medidas específicas para plataformas digitales dirigidas a menores.
¿Cómo evalúa el nivel de preparación de las entidades públicas y privadas en el cumplimiento efectivo de la normativa vigente sobre protección de datos?	Las entidades educativas y tecnológicas no tienen protocolos claros sobre consentimiento parental, tratamiento de imágenes ni uso de datos escolares.
¿Qué rol debería jugar la academia y la investigación jurídica en el diseño de futuras políticas públicas sobre seguridad digital y protección de datos en Ecuador?	La academia debe impulsar reformas legales que reconozcan el interés superior del menor también en el ecosistema digital y formar defensores especializados.

4. DISCUSIÓN

La normativa ecuatoriana proporciona un fundamento sólido para la protección de la información personal, determinando claramente los principios, derechos y obligaciones relacionadas con su tratamiento. Desde una perspectiva académica y profesional, este marco legal suscita diversos aspectos relevantes. Salvador (2022) destaca que el avance tecnológico en Ecuador ha incrementado notablemente la generación, procesamiento y almacenamiento de datos personales en diversas plataformas digitales, situación que genera retos significativos en cuanto a su seguridad. En este contexto, la Ley Orgánica de Protección de Datos Personales constituye un instrumento regulador clave para abordar estos desafíos. De esta forma, la ley salvaguarda los derechos de quienes son titulares de los datos y establece, al mismo tiempo, las obligaciones de las instituciones y organizaciones responsables de manejarlos.

La protección de la LOPD cumple con las normas internacionales y abarca el cuatro temas principales: consentimiento informado, salvaguarda de la privacidad, derechos de la persona en cuyos almacenamientos de datos se involucran, y movimiento internacional de datos. Por ejemplo, el artículo 11 del LOPD la obligación de obtener el consentimiento de la persona en cuestión para diversos usos de los datos, excepto en aquellos casos en que la legislación específicamente permita lo contrario (Ley Orgánica de Protección de Datos Personales, 2021). Otro ejemplo es el artículo 17, que estipula que una persona debe extender medidas adecuadas para proteger los datos de las personas contra la divulgación no autorizada o el uso indebido.

Existe un sistema jurídico sólido en Ecuador para garantizar la privacidad de los datos personales, ya que la seguridad de la información es un derecho humano fundamental y se impregna de intimidad. Dado que la Constitución otorga derechos fundamentales a cada persona, la protección de la privacidad juega un papel crucial en el escenario actual de una sociedad digital.

Así, en este sentido, la Ley Orgánica de Protección de Datos Personales, en vigor desde hace dos años, permite conceder a los ciudadanos los derechos y las responsabilidades en este ámbito a nivel de población y base general para el derecho a la privacidad de los ciudadanos ecuatorianos. No obstante, cabe mencionar que el desafío es la falta de conciencia y conocimiento acerca de este tema, en todo caso a la baja cantidad acceso y conocimiento de los ciudadanos acerca de este tema. El establecimiento requiere más cambios y adaptabilidad en relación con otras formas de operaciones tecnológicas y cibernéticas.

En cuanto a la protección de los datos personales, Heredia (2022) insiste en la obligación de mantener la privacidad de las constantes. Ello se logra mediante medidas y regulaciones legales que normalmente rigen sobre una clase designada de información, o sea, la que identifica a personas, sea presente en sistemas informáticos, soportes, registrados en bases de datos o informáticamente tratados. Entre los fines de la protección de datos destacan la determinación de qué formación se considerará personal, la identificación de quién es el responsable de dicho procesamiento y la definición de las reglas que regulan la formación, conservación, acceso, seguridad y confidencialidad de estos datos, así como la protección a nivel cualitativo adecuado incluso con respecto a la transferencia internacional de datos personales.

No obstante, se reconoce que aún persisten ciertas limitaciones y desafíos en esta área, tales como la ausencia de una definición clara sobre qué constituye exactamente un dato personal, así como la falta de normas específicas para regular su gestión en los ámbitos público y privado.

Por otro lado, de las entrevistas realizadas a expertos se determina la existencia de un consenso fundamental sobre las notables falencias del país en materia de protección de datos personales. Si bien la aprobación de la Ley Orgánica de Protección de Datos Personales en 2021 constituyó un avance crucial en términos normativos, los especialistas opinan que su aplicación actualmente es muy restringida y sufre una serie de limitaciones en los campos institucional, técnico y cultural. Si bien esta ley toma como referencia estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de Europa, en la práctica carece de un respaldo institucional sólido que permita asegurar su cumplimiento efectivo, especialmente considerando que el país aún enfrenta dificultades para fortalecer sus instituciones democráticas.

Desde la perspectiva constitucionalista, claramente hay una brecha entre la letra de los principios garantistas de la Constitución ecuatoriana y la forma en que realmente se protegen los derechos digitales. Aunque la autodeterminación informativa está protegida implícitamente, su regulación legal es deficiente, y todavía no existen precedentes judiciales que se pueda citar en relación con ella. En el ámbito penal, la brecha encontrada fue que claramente hay una falta de conexión entre la normativa de protección de datos personales y el sistema penal, ya que no hay ninguna disposición sobre el robo de identidad digital y la venta ilegal de datos personales.

Por otro lado, a nivel institucional, la situación no es más alentadora, ya que las recomendaciones antidopaje recalcan que en general, “las entidades públicas no están listas para los retos mínimos en términos del manejo de los datos”. Muchas instituciones carecen de personas específicamente designadas para la protección de datos, no tienen políticas internas actualizadas y, en ocasiones, no saben de qué se espera de ellos. Además, la falta de recursos, personal formado y el desinterés por parte de las autoridades competentes resulta en que la legislación existente no se tome en serio y no tenga un impacto significativo, lo que lo convierte en una mera formalidad.

Si se considera una mirada comparativa, el RGPD europeo estándar representa uno de los estándares más avanzados en términos normativos e institucionales y puede ser un estándar facilitador para su implementación en otros países. La importancia radica en la responsabilidad

proactiva y la necesidad de realizar evaluaciones de impacto en la protección de datos antes del tratamiento y la autoridad independiente designada para controlar el cumplimiento de los códigos. Algunos de los componentes aún no codificados en el marco legal de Ecuador tienen el potencial de reforzar significativamente la protección de datos en Ecuador. Además, el principio del RGPD basado en la "privacidad desde el diseño" puede servir como una buena práctica para fortalecer la política local de regulación.

Un área crítica que ilustra la falta de protección adecuada de los derechos de datos personales de un grupo vulnerable en la legislación ecuatoriana es el de los niños, niñas y adolescentes en el contexto digital. En contraste, el RGPD proporciona otras salvaguardias, como la obligación del consentimiento del titular de la patria potestad y la creación de plataformas digitales seguras para los niños, mientras que el marco ecuatoriano no contiene enmiendas adicionales. Dado que las disposiciones actuales en la legislación local no son suficientes, este vacío representa un desafío apropiado, ya que infringe los principios constitucionales del interés superior del niño y de la protección integral de un niño.

Ecuador se encuentra en un momento de transición normativa, y la mera existencia de una ley de protección de datos no asegura su aplicación efectiva. Dado este escenario, la comparación frente al RGPD no solo ha permitido identificar carencias, sino que traza posibles soluciones. Dado el marco teórico y práctico anterior, subrayar la necesidad de contar con una autoridad verdaderamente autónoma, la transparencia de políticas públicas, el establecimiento de sanciones efectivas y la educación digital, aunque puedan ser repetitivas, son acciones cruciales para avanzar hacia una protección de datos personales más sólida, respetuosa de los derechos fundamentales y acorde a los estándares internacionales más exigentes.

Sin embargo, la Ley Orgánica de Protección de Datos Personales (2021) ofrece disposiciones claras en el tema de protección de los mismos. Cualquier operación que se realice sobre datos personales podrá estar sometida mediante procedimientos técnicos automatizados, parcialmente automatizados o manuales, cubriendo con igualdad de forma el ordenamiento las definiciones que comprenden: operaciones de recolección, obtención, registro, organización, almacenamiento, resguardo, adaptación, modificación, supresión, indexación, extracción, consulta, procesamiento, uso, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia y cualquier otra que implique acceso, comparación, interconexión, limitación o

destrucción de datos personales, lo que de por sí comprende cualquier modalidad de tratamiento de información personal.

5. CONCLUSIÓN

En Ecuador, hay fuertes marcos legales destinados a garantizar la protección de los datos personales, consagrados en la Constitución y la Ley Orgánica de Protección de Datos Personales. Estos marcos legales definen explícitamente los derechos, principios y obligaciones que deben observar todas las entidades al procesar información personal, con el fin de proteger la privacidad del ciudadano común.

Sin embargo, a pesar de tener un sólido marco jurídico, uno de los principales problemas radica en que, al implementarse, no se llevan a la práctica real estas normativas, principalmente debido a la falta de conciencia social sobre la importancia de la protección de datos y la velocidad con la que la legislación debe adaptarse a los avances tecnológicos. Por lo que es necesario que las autoridades e incluso la sociedad misma trabajen para impulsar la cultura de información cuidada y con ella una aplicación efectiva de las leyes.

Las entrevistas indican que, si bien personal del Ecuador implementó la Ley Orgánica de Protección de Datos Personales, hay problemas significativos en la práctica. Los expertos informaron que las agencias carecen de recursos técnicos y profesionales adecuados y, por lo tanto, no se entiende la idea de los datos como un derecho humano fundamental. Finalmente, es relevante destacar que, debido a la débil institucionalidad y la escasa cultura jurídica digital del país, incluso la ley no otorga protección suficiente frente a los riesgos inherentes al actual entorno digital. En otras palabras, la regulación no asegura los derechos de los ciudadanos en el ámbito de datos personales.

En esta situación, el Reglamento General de Protección de Datos de Europa incluye puntos valiosos para postular una legislación más fuerte en Ecuador. Algunos de los aspectos fundamentales para reacondicionar en el marco civil ecuatoriano se encuentran el enfoque hacia la responsabilidad activa de las entidades procesadoras, la necesidad de llevar a cabo evaluaciones de riesgos ante posibles filtraciones y la posibilidad de contar con organismos sancionatorios externos apegados a la falta de dependencia. Es igual de importante resaltar la importancia de estas medidas y sus aportes en el marco de la formación de políticas públicas y

campañas de formación sobre la importancia de proteger la concesión de información personal para crear un marco más sólido, eficaz y actualizado con las leyes internacionales.

6. REFERENCIAS BIBLIOGRÁFICAS

Asamblea Nacional. (2021). Ley Orgánica de Protección de Datos Personales. Quito, Ecuador.

Cevallos, A. (2021). La divulgación y el uso irregular de los datos personales en Ecuador. *Repositorio Universidad de Guayaquil*. Obtenido de http://repositorio.ug.edu.ec/handle/redug/57932

Guerrero, B. G. (2020). Protección de datos personales en el Poder Judicial: Una nueva mirada al principio de publicidad de las actuaciones judiciales. *Scielo* , 33-56.

Jurado, Z. E., Riera, L. E., & Méndez, J. A. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. *Polo del Conocimiento*, 1355-1373. doi:https://doi.org/10.23857/pc.v8i8.5908

Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. *Technology Rain Journal*. doi:https://doi.org/10.55204/trj.v2i2.e17

Segarra, E. (2011). Derecho a la intimidad. Análisis a la normativa ecuatoriana. *Repositorio Institucional Universidad de Azuay*. Obtenido de http://dspace.uazuay.edu.ec/handle/datos/5520

Constitución de la República de Ecuador. (20 de octubre de 2008). Registro Oficial 449. *Asamblea Nacional del Ecuador*. Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Barreto, W. E. (2023). Protección de datos personales en Ecuador a consecuencia de la emergencia sanitaria Covid-19. *Revista Universidad y Sociedad*. Obtenido de http://scielo.sld.cu/scielo.php?pid=S2218-36202023000200194&script=sci_arttext&tlng=en

Martínez, M. R., López, J. A., Cevallos, D. P., & Burgos, G. P. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 369-382. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8641863

Pineda, L. O., & Quezada, C. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*. Obtenido de https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Carrillo, F. N. (2022). Los ejes centrales de la protección de datos: consentimiento y finalidad. *USFQ Law Review*, 2-175. doi:https://doi.org/10.18272/ulr.v8i1.2184

Vivar, S. A., Ochoa, N. V., Guamán, C. R., & Molina, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y*

Sociedad. Obtenido de http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt

Martínez, G. E., Plúas, Y. G., & Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, 46-64. doi:https://doi.org/10.55813/gaea/jessr/v4/n3/113

Argudo, M. A., Pinos, J. M., & Mora, M. F. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 100-114. Obtenido de https://www.proquest.com/openview/d29c2f8f2bdc11ccd4644ff0be3d8b56/1?pq-origsite=gscholar&cbl=1006393

Reglamento General de Protección de Datos. (4 de mayo de 2016). Gazzetta ufficiale dell'Unione europea. *„Journal officiel de l'Union européenne, L 119*. Obtenido de https://eu.vlex.com/vid/regulation-eu-2016-679-843418428?from_fbt=1&forw=go&fbt=webapp_preview&addon_version=6.9

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. *Registro Oficial Suplemento 180*. Quito, Ecuador. Obtenido de Obtenido de: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Salvador, W. (2022). Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicos en vícimas ecuatorianas. *Revista mundo financiero. Volumen 3.*, 45. Obtenido de http://www.mundofinanciero.indecsar.orgDerecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicosenvíctimas ecuatorianasThe right to privacy and cybercrime. Social and economic effects on Ecuadorian victimsWashington Manuel Salvador Quiñ

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). Proyecto de la Unión Europea para Resiliencia Cibernética para el. *Estrategia Nacional de Ciberseguridad*. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf

Heredia, J. S. (2022). Ciberseguridad en Ecuador. *Revista Killkana*. doi:https://doi.org/10.26871/killkanatecnica.v5i1.957