UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD DE CIENCIAS SOCIALES, DERECHO Y BIENESTAR
CARRERA DE DERECHO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA DEL ECUADOR

TITULO:

"EL IMPACTO DEL RGPD EN LAS POLÍTICAS Y PRÁCTICAS DE PROTECCIÓN DE DATOS EN ECUADOR."

AUTOR:

GARCÍA ROLDÁN JACK ELLIAN

DOCENTE TUTOR:

DR. JAVIER ESPINOZA SUÁREZ

MANTA, JUNIO DE 2024

CERTIFICADO DE TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Facultad Ciencias Sociales Derecho y Bienestar de la carrera de Derecho de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría del estudiante García Roldan Jack Ellian , legalmente matriculado en la carrera de Derecho, período académico 2024-1, cumpliendo el total de 384 horas, cuyo tema del proyecto es "**El impacto del RGPD en las prácticas y políticas de proteccion de datos en Ecuador**".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Lugar, 14 de junio de 2024

Lo certifico,

JAVIER ANDRES ESPINOZA SUAREZ

Firmado digitalmente por JAVIER ANDRES ESPINOZA SUAREZ
Fecha: 2024.06.14 10:38:31 -05'00'

Abg. Javier Espinoza Suárez, Mg.
Docente Tutor(a)
Área: Derecho Informático

DECLARACION DE AUTORIA

Declaración de Autoria

El trabajo de grado denominado **"EL IMPACTO DEL RGPD EN LAS POLÍTICAS Y PRÁCTICAS DE PROTECCIÓN DE DATOS EN ECUADOR"**, ha sido desarrollada con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan en las páginas correspondientes, cuyas fuentes de incorporan en la bibliografía.

En virtud de esta declaración me responsabilizo del contenido, veracidad y alcance científico de proyecto de grado en mención.

García Roldán Jack Ellan

AGRADECIMIENTO

A mis padres, que han estado apoyándome desde siempre para poder ser un gran profesional y también un mejor ser humano; siempre contando con su incondicionalidad en los momentos más difíciles.

A mis queridos abuelos, que han sido como unos segundos padres para mí y pilares importantes en mi vida; brindándole calidez a mi ser.

A mis queridos amigo y a todas las personas que han sido parte importante de mi vida y crecimiento.

DEDICATORIA

A Yolanda y María Eugenia, pilares en mi vida,
mi sol y cielo.

RESUMEN

Este estudio investigó el impacto del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en las políticas y prácticas de protección de datos en Ecuador. Se analizó cómo la normativa europea ha influido en la creación y aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP), identificando similitudes, diferencias y desafíos en su implementación. A través de un análisis comparativo, se examinaron los cambios normativos y su impacto en empresas y organismos ecuatorianos que manejan datos personales. También se evaluaron las sanciones y consecuencias del incumplimiento de estas regulaciones. Los hallazgos indican que, si bien la LOPDP representa un avance significativo en la protección de datos en Ecuador, aún enfrenta retos en su aplicación y supervisión. Finalmente, el estudio propone recomendaciones para mejorar la adecuación de la normativa ecuatoriana a estándares internacionales y fortalecer la seguridad jurídica y la confianza en el entorno digital del país.

Palabras Claves: protección de datos, rgpd, lopdp, legislación ecuatoriana
impacto normativo

ABSTRACT

This study investigated the impact of the European Union's General Data Protection Regulation (RGPD) on data protection policies and practices in Ecuador. It analyzed how the European regulation has influenced the creation and application of the Organic Law on Personal Data Protection (LOPDP), identifying similarities, differences and challenges in its implementation. Through a comparative analysis, the regulatory changes and their impact on Ecuadorian companies and organizations that handle personal data were examined. The sanctions and consequences of non-compliance with these regulations were also evaluated. The findings indicate that, although the LOPDP represents a significant advance in data protection in Ecuador, it still faces challenges in its application and supervision. Finally, the study proposes recommendations to improve the alignment of Ecuadorian regulations with international standards and to strengthen legal certainty and trust in the country's digital environment.

Keywords: data protection; rgpd; lopd; ecuadorian legislation; regulatory impact

Contenido

INTRODUCCIÓN

En una época cada vez más interconectada y digital, la protección de los datos personales se ha convertido en una cuestión de suma importancia a nivel mundial. En consecuencia, entes internacionales como La Organización de Naciones Unidas (ONU), La Organización de Estados Americanos (OEA), así como la Comisión Europea, han sido los pioneros en el desarrollo de legislaciones con relación a los datos personales, desembocando este último en el RGPD.

Es así, que la Comisión Europea indica que los datos personales se pueden definir como cualquier información relacionada con una persona física viva que esté identificada o que pueda ser identificable, del mismo modo cualquier información recopilada que pueda contribuir a la identificación de una persona también se considera como datos personales. (Aguilar et al., 2022).

Si bien el RGPD ha servido como modelo referente y más para Ecuador, este último aún enfrenta desafíos específicos en la necesidad de educar al público y a las propias empresas sobre sus derechos y responsabilidades, así como de desarrollar la infraestructura necesaria para asegurar el cumplimiento del mismo lo que resulta en tareas cruciales, es por ello que la autoridad de protección de datos en Ecuador debe realizar esfuerzos significativos para supervisar y hacer cumplir la nueva legislación.

Ordóñez et al., (2022) indica lo siguiente:

> En Ecuador la protección de los datos personales ha evolucionado en tres etapas principales, inicialmente, se estableció la protección a través del habeas data en la constitución. Para después implementar leyes sectoriales que regulasen la información personal y la intimidad desde una perspectiva garantista, en la tercera etapa fue el reconocimiento de la protección de datos personales como un derecho fundamental en la Constitución de 2008. Sin embargo, con la promulgación de la ley orgánica de protección de datos (LOPD) en 2021, se inició una cuarta etapa en la que, desde la perspectiva constitucional ecuatoriana, la protección de los bienes jurídicos relacionados

> con la protección de datos en la era digital cobra una especial relevancia debido a la variedad de medios disponibles para la difusión de datos personales y las posibles intromisiones ilegítimas que pueden ocurrir sin el consentimiento del titular de dichos datos. (pág. 79)

A raíz de esto podemos concluir que Ecuador ha mostrado una capacidad de ajuste en cuanto a la gestión de datos personales, adaptándose a diferentes contextos en cada una de estas áreas, esto resalta la relevancia de resguardar los intereses legales asociados con la protección de datos en la era digital, considerando la amplia gama de plataformas de difusión y los potenciales riesgos de intromisión sin el consentimiento del titular de la información.

Por lo mismo, la implementación de normas y prácticas alineadas con el RGPD está ayudando a Ecuador a integrarse mejor en la economía digital global, del mismo modo que las empresas ecuatorianas que manejan datos personales de ciudadanos europeos deben cumplir con el RGPD, lo que exige una armonización de prácticas y políticas de protección de datos, esta alineación hace que se faciliten el comercio y la cooperación internacional, al proporcionar un marco regulatorio que las empresas extranjeras consideran fiable, siendo así innegable su impacto.

El cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador no solo evita multas financieras, sino que también fortalece la reputación corporativa y genera confianza entre clientes y empleados, por consecuente, las organizaciones que cumplen con esta normativa pueden optimizar sus operaciones mediante aplicaciones empresariales, lo cual mejora la eficiencia en las tareas, facilita un mejor control estadístico y permite economizar tiempo y recursos.

CAPÍTULO 1: DISEÑO TEORICO

1.1. JUSTIFICACIÓN DE LA INVESTIGACIÓN

La presente investigación se justifica por la necesidad de comprender el impacto del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en las políticas y prácticas de protección de datos en Ecuador, en un contexto global marcado por un creciente interés en la tutela de la información personal. A pesar de la relevancia del tema, existe una notable escasez de estudios que analicen en profundidad este impacto en el ámbito ecuatoriano. Los resultados de esta investigación tienen el potencial de beneficiar significativamente a diversos actores clave, incluyendo al gobierno, las empresas y otros organismos relevantes en materia de protección de datos.

La información obtenida proporcionará una guía valiosa para realizar los cambios necesarios a fin de cumplir con los estándares del RGPD y, en consecuencia, fortalecer la protección de datos en el país.

A medida que Ecuador avanza en la regulación de la protección de datos con su Ley Orgánica de Protección de Datos Personales (LOPDP), es fundamental investigar el impacto que ha tenido el RGPD en las prácticas y políticas locales, esta investigación resulta crucial para comprender las adaptaciones y desafíos a los que se enfrentan las instituciones ecuatorianas al adoptar estándares internacionales, además, permite evaluar la efectividad y adecuación de la LOPDP en la protección de los datos personales, comparándola con el RGPD. El estudio también servirá como punto de referencia para mejorar las políticas nacionales, fomentando una cultura sólida de protección de datos alineada con las mejores prácticas a nivel mundial. De esta manera, se contribuirá al fortalecimiento de la seguridad jurídica, la confianza ciudadana y el desarrollo sostenible del entorno digital en Ecuador, adicionalmente, esta investigación contribuirá al avance del conocimiento académico en el campo de la protección de datos en Ecuador, particularmente en lo que respecta a la influencia de normativas internacionales como el RGPD en las políticas y prácticas locales.

Este estudio aportará al conocimiento académico y práctico en el área de la protección de datos, estableciendo una base sólida para investigaciones futuras y avances legislativos. Además, ayudará a los tomadores de decisiones, empresas y ciudadanos a comprender mejor los desafíos y oportunidades que implica la protección de datos en la era digital. La importancia de esta investigación radica en su potencial para mejorar la protección de los datos personales en Ecuador, garantizando que el país siga los estándares internacionales más destacados y fomente un entorno digital seguro y confiable para todos sus habitantes. Se analizará si la Ley Orgánica de Protección de Datos Personales (LOPDP) ofrece una protección adecuada de los datos personales y cómo se compara con la rigurosidad del Reglamento General de Protección de Datos (RGPD).

1.2. OBJETIVO DE LA INVESTIGACIÓN

Esta investigación tiene como objetivo principal analizar el impacto del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en las políticas y prácticas de protección de datos en Ecuador. Se busca comprender en profundidad cómo la entrada en vigor del RGPD ha influenciado las normativas, procedimientos y medidas adoptadas por el gobierno ecuatoriano, las empresas y otros actores relevantes en materia de protección de datos personales.

Para cumplir con este objetivo, se realizarán análisis comparativos, en los que se detallarán las similitudes y diferencias entre el RGPD y la LOPD relacionadas con las definiciones, principios, derechos de los titulares de datos y obligaciones de los responsables y encargados, de igual manera, los estudios de caso se implementarán en varias instituciones de Ecuador para evaluar su preparación para la aplicación de la LOPD y la influencia del RGPD en sus actividades. Los aspectos que se considerará son la tecnología digital, la educación del personal y las regulaciones internas que supervisan la gestión de datos. Por último, se analizarán los datos tanto cuantitativos como cualitativos, incluidas encuestas de especialistas en protección de datos y entrevistas con representantes de agencias gubernamentales y otros organismos, así como propietarios de datos.

Al final, este estudio proporcionará una valiosa comprensión académica y práctica de la protección de datos, lo que dará como resultado un mundo digital seguro y confiable para todos los ciudadanos del Ecuador

Por lo tanto, revelar los desafíos y oportunidades que enfrentan en la protección de datos personales y evaluar la influencia del reglamento de datos en el país en términos de confianza ciudadana y seguridad jurídica en el Ecuador, además, con el objetivo de mejorar las políticas públicas de protección de datos del país, se formularán recomendaciones basadas en los resultados de la investigación actual.

1.3. PLANTEAMIENTO DEL PROBLEMA

La promulgación del Reglamento General de Protección de Datos (RGPD) de la Unión Europea ha marcado un hito en el panorama global de la protección de datos. Si bien Ecuador no pertenece a la UE, el RGPD posee un alcance extraterritorial que impacta en las políticas y prácticas de protección de datos del país.

En la era actual, la salvaguardia de la información personal ha adquirido una inmensa importancia a nivel mundial, ya que es crucial para defender la privacidad y la seguridad de las personas. El reglamento general de protección de datos, que tiene su sede en la unión europea, se ha convertido en un estándar global, influyendo en la legislación de diferentes regiones del mundo. Para dar cumplimiento a estas normas, el ecuador ha implementado la ley orgánica de protección de datos personales, no obstante, es fundamental examinar la implementación y adaptación de esta directriz en el país, y cómo ha influido en las prácticas y políticas de protección de datos tanto en el sector público como en el privado. La principal preocupación es el nivel de eficacia y adecuación de la LOPD en relación con el RGPD, es de suma importancia, el examen de los estándares internacionales en la legislación ecuatoriana y la recepción de la legislación por parte de las instituciones pertinentes responsables de salvaguardar la información personal. Por ende, identificar los obstáculos que enfrentan estas organizaciones para cumplir con las nuevas regulaciones, así como las posibilidades de mejorar la seguridad de los datos en Ecuador.

Este reglamento establece estándares rigurosos para la protección de datos personales, exigiendo a las empresas y organizaciones ecuatorianas que manejan información de ciudadanos de la UE que acaten sus disposiciones. En consecuencia, ha surgido la necesidad de que Ecuador revise y adapte sus políticas y prácticas de protección de datos para ajustarse al estándar de protección de derechos a nivel mundial. Esto ha impulsado cambios en las normativas, procedimientos y medidas adoptadas por el gobierno, las empresas y otros actores relevantes en materia de protección de datos personales en Ecuador.

1.4. FORMULACIÓN DEL PROBLEMA

¿En qué medida ha impactado el Reglamento General de Protección de Datos (RGPD) de la Unión Europea en las políticas y prácticas de protección de datos en Ecuador?

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Analizar el impacto del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en las políticas y prácticas de protección de datos en Ecuador.

1.5.2. OBJETIVO ESPECIFICOS

- Identificar los principales desafíos y oportunidades que la elevada protección de derechos del RGPD ha presentado para el gobierno y demás actores relevantes en el ámbito de la protección de datos en Ecuador.
- Analizar las modificaciones legislativas y regulatorias que se han llevado a cabo en Ecuador como resultado de la entrada en vigor del RGPD.
- Analizar cómo el RGPD ha influido en la forma en que las organizaciones ecuatorianas manejan la información personal.

1.6. METODOLOGÍA

Los métodos de investigación que han sido utilizados durante la elaboración del presente trabajo de investigación son: método analítico, método bibliográfico, método histórico Lógico

- **Método analítico. -** Se caracteriza en descomponer un objeto o fenómeno en sus partes más simples para comprender mejor su funcionamiento. Este método de investigación busca aislar y examinar cada componente con el fin de obtener una visión más compleja del fenómeno de estudio para identificar patrones, relaciones y mecanismos casuales que pueden pasar desapercibidos (Gomez, 2019)**.**
- **Método bibliográfico. -** Se especifica en la acción de investigar fuentes de información de origen del libro, artículos científicos y leyes con el fin de obtener un sustento para la investigación (Clavijo, 2021).
- **Método histórico – lógico. -** Para este método se complementan dos métodos dentro de uno solo, el método histórico realiza un estudio de la trayectoria de los acontecimientos y los fenómenos dentro de determinado periodo de tiempo; y el método lógico investiga el desarrollo de los fenómenos y las leyes del funcionamiento de estos.

CAPÍTULO 2: MARCO TEÓRICO

2.1. ANTECEDENTES DEL RGPD

El Reglamento General de Protección de Datos (de aquí en adelante RGPD) de la Unión Europea, o también conocido como Reglamento 2016/679, surge a través de la aprobación del Parlamento Europeo y el Consejo de la Unión Europea, entrando en vigor en mayo del 2016, y de los dos años posteriores de su vigencia para las empresas, organismos, organizaciones y/o instituciones del sector para que pudieran adaptar esta norma dentro de sus procesos a esta norma en aplicación plena desde el 25 de mayo de 2018 (UNIR REVISTA , 2021).

Este Reglamento es originario, como lo expone la Comisión Europea como una herramienta y medida esencial en la que se pueda reforzar los derechos fundamentales de las personas en un mundo digitalizado, de forma que se facilite la actividad económica. Su propósito es la de servir esta normativa como base aclaratoria de las normas aplicables hacia las empresas y organismos públicas en el mercado único digital.

A su vez, la creación de este Reglamento es impulsado por el contexto europeo, debido a que la carencia de legislaciones europeas dentro del concepto de protección de datos se encontraba faltante de regulaciones legales, aspecto preocupante para las Naciones Europeas en el continente, originándose así un margen legal corregidor de carencias en derechos de protección digitales definidos imperativamente en un propio ámbito de aplicación.

Al existir una única norma para la protección de datos personales en el bloque europeo, se interpone un sistema fragmentado por el cual se corregían los formatos de suma de trámites varios y de cargas administrativas innecesarias en paradigmas del regulador europeo.

Así, como lo establece la norma, se trata de una norma de aplicación directa y obligatoria de cada Estado miembro. Para el contexto de España, la vigencia del RGPD supondría una derogación de su predecesor, la Ley Orgánica de Datos de Carácter Personal del año 1999: así de este modo, el Gobierno español para poder

adoptar a la normativa nacional vigente el RGPD necesariamente tuvo que aprobar la Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPD-GDD) (Nisa Ávila, 2020).

2.1.1. ORIGEN Y OBJETIVOS DEL RGPD

El Reglamento General de Protección de Datos o Reglamento (UE) 2016/679 es una ley europea concerniente a la protección de datos digitales de las personas físicas, esto independientemente de si se tratan de ciudadanos que conforman la Unión Europea, en base al tratamiento y garantía de derechos de sus datos personales y de libre circulación de los mismos en la Unión Europea y el Espacio Económico Europeo (EEE), siendo parte fundamental como componente de la legislación europea priorizando la privacidad y defensa de los derechos humanos, en énfasis especial del artículo 8, apartado 1ro, de la Carta de los Derechos Fundamentales de la Unión Europea, así como de abordar la transferencia de datos personales ajenos de la UE y de apartados de las zonas del EEE (Google Spain SL, 2019).

Es publicado dentro del Diario Oficial de la Unión Europea el 4 de mayo de 2016, entrando en vigor 20 días después y siendo aplicado el 25 de mayo de 2018, dos años después para su adecuada implementación en empresas e instituciones.

Su objetivo principal como lo establece la Directiva 95/46/CE (2016) del Parlamento Europeo y del Consejo es la de tratar de armonizar la protección de derechos y de las libertades fundamentales de personas físicas en relación con actividades del espacio de tratamiento de datos de carácter personal, para garantizar la libre circulación de los datos entre Estados miembros (Parlamento Europeo y Consejo de la Unión Europea, 2016, pág. 1).

2.1.2. PRINCIPALES DISPOSICIONES DEL RGPD

El RGPD (Parlamento Europeo, 2016) establece en su Capítulo I, por disposiciones generales cuatro artículos a tomar en consideración tales como los siguientes:

Artículo 1.: los principales objetivos de este reglamento son los de: a) establecer normas de protección a personas físicas sobre tratamientos de sus datos

personales y de las normas de libre circulación de los mismos; b) proteger los derechos y libertades de aquellas personas físicas, y por sobre todo de sus derechos de protección en datos personales; y, c) en lo concerniente a la protección de estos mismos derechos, la Unión Europea no puede prohibir o restringir la libre circulación de datos personas en derechos resguardados a las personas físicas (pág. 1).

Artículo 2.: dentro del ámbito de principio de aplicación de este Reglamento se establecen cuatro apartados esenciales como lo son: 1) es aplicable las normas del Reglamento en tratamientos totales o parciales de manera automatizada en datos personales, así como de aquellos no automatizados pero contenidos o direccionados hacia un fichero. 2) No se aplicará las normas del Reglamento en los casos de ejercicio de un acto no comprendido dentro del ámbito aplicable del Derecho de la Unión Europea, por parte de los Estados miembros en actos comprendidas en el siguiente capítulo segundo, titulo V del TUE, por efectos de persona física por motivos de exclusividad personal o doméstica, y por autoridades en razones de prevención, investigación, detección o juicio de infracción en tipo penal o por sanciones penales. 3) Serán aplicables el Reglamento (CE) 45/2001 por motivos de carácter personal en instituciones y demás organismos de la Unión Europea, mientras que de actos jurídicos de la Unión se aplicarán encaminados a los principios y normas del RGPD conforme lo establece el artículo 98. 4. No será entendido por perjuicio la aplicación por la Directiva 2000/31/CE en especial de las normas de responsabilidad de prestadores de servicios intermedios conforme el artículo 12 al 15 (pág. 1).

Artículo 3.: de acuerdo con el principio de aplicación territorial del RGPD, se logra comprender tres esenciales numerales: 1) Será aplicado por ámbito territorial el presente Reglamento al tratamiento de datos personales de personas físicas por un establecimiento encargado de la Unión Europea, sin perjuicio de que tenga lugar o no de un tratamiento en la Unión Europea. 2) Será aplicado el tratamiento de datos personales por parte interesada o responsable en casos de ofertas de bienes o servicios independientes de su pago o por control de comportamiento con cabida

de la Unión Europea. 3) Será aplicada la normativa del RGPD en Estados miembros por Derecho Internacional público (pág. 2).

Artículo 4.: al tratarse el Reglamento 2016/679 de una normativa con aplicación internacional, este artículo enmarca las definiciones y delimitaciones de palabras claves que se embarcan en el presente cuerpo normativo como lo es “tratamientos” al momento de referirse a toda forma automatizada o no automatizada de operar un conjunto de datos personales de las personas físicas en su registro, extracción, empleo, conservación, entre otros (pág. 2).

2.2. LEGISLACIÓN DE PROTECCIÓN DE DATOS EN ECUADOR

Nuestro país es un estado constitucional de derechos y justicia, donde se garantiza el goce efectivo de los derechos establecidos en su norma suprema e instrumentos internacionales, la Constitución de la República del Ecuador de 2008 en su artículo 66, numeral 19, establece el derecho a la protección de datos personales, incluyendo la facultad de decidir y acceder a la información, así como su protección, este derecho exige que el titular de los datos autorice legalmente la recolección, procesamiento, distribución, difusión y archivo antes de cualquier tratamiento. La normativa interna regula este derecho constitucional, cuya violación puede resultar en acciones judiciales, civiles o penales (Constitución de la República del Ecuador, 2008).

Es decir, todas las personas son iguales y gozan de las mismas oportunidades incluyendo la protección de datos, que permite a las personas conocer, acceder, solicitar cambios o eliminación de información en fuentes físicas o digitales, y demandar a la parte infractora por el uso no consentido de sus datos.

Dicho esto, la legislación vigente en materia de protección de datos personales si bien no es escasa, su normativa puede referirse a tres elementos esenciales de los cuales permiten regular el registro de datos personales, otra encargada de establecer acciones jurídicas orientadas a su rectificación o modificación, y por último de aquella con carácter penal, puesto que sanciona su interceptación y difusión siguiente. Con ello, se hace referencia a la Ley del Sistema Nacional de Registro de Datos Públicos (LSNRDP), la Ley Orgánica de Garantías

Jurisdiccionales y Control Constitucional (LOGJCC), y del Código Orgánico Integral Penal (COIP), respectivamente (Córdova Hidalgo, 2020).

Sin embargo, cabe resaltar la relevancia y vigencia en la materia entendida que tiene una relativamente nueva legislación ecuatoriana como lo es la Ley Orgánica de Protección de Datos Personales (LOPD) con fecha de publicación en el Registro Oficial 459 del 26 de mayo de 2021, además del reglamento a la ley de Protección de Datos Personales publicado en 2023 con la finalidad de brindar una idónea protección de datos como derecho primordial frente al suscitado avance tecnológico, para fortalecer la seguridad jurídica.

El Embajador de Ecuador ante la Unión Europea, Charles-Michel Geurtse, destacó que la protección de datos es esencial para una sociedad informada sobre sistemas de información. Geurtse afirmó que la implementación de esta legislación en Ecuador se suma a los esfuerzos de otros países latinoamericanos en el proceso de digitalización global, con un énfasis especial en la cooperación bilateral y multilateral promovida por la Unión Europea. (Alvear & Pesantes, 2023)

La Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador establece directrices generales que tanto las instituciones públicas como privadas deben cumplir, aplicándose a domiciliados y no domiciliados que manejen datos de residentes ecuatorianos, al igual que designa una autoridad máxima para supervisar y asegurar el cumplimiento de la ley, con la capacidad de resolver reclamaciones y aplicar sanciones en caso de incumplimiento. La ley introduce conceptos como el responsable, encargado y delegado del tratamiento de datos, definiendo roles específicos para la protección y manejo de la información personal (Ley Orgánica de Protección de Datos Personales, 2021).

2.2.1. MARCO LEGAL EXISTENTE ANTES DEL RGPD

Antes de la aprobación y desarrollo de la Ley Orgánica de Protección de Datos del Ecuador, la protección de datos personales se mencionaba en diversos artículos y leyes, incluyendo la Constitución de la República del Ecuador de 2008 (arts. 66, 92), la Ley N.º 162 del Sistema Nacional de Registro de Datos Públicos, la Ley N.º 13 de Burós de Información Crediticia (arts. 5 a 10), la Ley N.º 67 de Comercio Electrónico, Firmas y Mensajes de Datos (art. 9), la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley N.º 184 Especial de Telecomunicaciones (arts. 1, 14, 39), la Ley Orgánica de Transparencia y Acceso a la Información (LOTAIP), el Código Orgánico Penal (COIP) (art. 178), la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (arts. 49, 50, 51), el Reglamento de Clasificación de Información Reservada y Confidencial de la Defensoría Pública de 2018 (art. 2) y la Guía de Tratamiento de Datos Personales en Administración Pública (art. 2).

Ecuador fue uno de los pocos países en América Latina que no tenía una ley especializada en protección de datos personales. Después de un significativo retraso que abarcó alrededor de 20 meses desde la presentación del proyecto de ley hasta su trámite y aprobación, el 26 de mayo de 2021 se publicó en el Registro Oficial N°59 la Ley Orgánica de Protección de Datos Personales (LOPDP), la cual entró en vigor inmediatamente, excepto por el régimen sancionador y correctivo que se implementará dos años después de su publicación. (Alvear & Pesantes, 2023)

Hasta la aprobación de la Ley Orgánica de Protección de Datos del Ecuador, no existía una regulación clara sobre la protección de datos personales, la cual se encontraba dispersamente regulada en varios cuerpos normativos. Entre estos, se incluía la Constitución de la República del Ecuador en su artículo 66, la Ley Orgánica de Telecomunicaciones, y el Código orgánico integral penal. Además, la disposición constitucional del “Habeas Data” también hacía referencia a la protección de datos personales. La Ley Orgánica de Telecomunicaciones en sus artículos 23 #4, 24 #14, 76, 77, 78 #2, #3 y #4, 79 y 82, así como la Ley Orgánica de Comunicación en sus

artículos 30 y 31, también contenían disposiciones sobre esta materia. (Alvear & Pesantes, 2023)

Integralmente, el Código Orgánico Integral Penal aborda la protección de datos en sus artículos 178, 180, 229 y 475, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos lo hace en sus artículos 5, 9, 48 y 49. También la Ley del Sistema Nacional de Registro de Datos Públicos regula este aspecto en sus artículos 4, 5 y 6, y la Ley Orgánica de Transparencia y Acceso a la Información Pública en sus artículos 2, 6 y 22, también contienen disposiciones relevantes sobre la protección de datos.

Añadido a este panorama, al comienzo de época de pandemia en Ecuador, la declaración del Estado en Estado de Emergencia en el país se dispuso la implicación de plataformas satelitales y telefónicas móviles con motivos de monitoreo en ubicación de personas por estado de cuarentena sanitaria y aislamiento obligatorio, así tras algún tipo de restricción o incumplimiento a la norma, se dispondría acciones legales frente a las autoridades judiciales y administrativas en competencia plena (Paz Canales & Bordachar, 2021).

En vista a esto con el aumento de la digitalización debido al trabajo remoto y la educación en línea, el gobierno y las organizaciones tuvieron que fortalecer las medidas de ciberseguridad para proteger los datos personales contra posibles brechas y ciberataques. La experiencia de la pandemia resaltó la importancia de tener marcos robustos de protección de datos que puedan adaptarse rápidamente a situaciones de emergencia sin comprometer la privacidad de los individuos. Además, subrayó la necesidad de invertir en infraestructura tecnológica y ciberseguridad, así como de fomentar la transparencia y la comunicación efectiva con el público para mantener la confianza y cooperación ciudadana, a su vez la necesidad urgente de implementar medidas para controlar la pandemia a veces podía entrar en conflicto con los marcos legales existentes de protección de datos.

Del mismo modo en la sentencia No. 2064-14-EP/21 de 2021, el tribunal resolvió una Acción Extraordinaria de Protección en la cual se afirmó que la decisión de apelar la denegación de la acción de hábeas data por parte de una mujer, cuyas fotos íntimas fueron reveladas sin su consentimiento, violó su derecho al acceso

efectivo a la justicia y al debido proceso, además el tribunal afirmó que se garantizará una opción inversa adecuada para la denunciante, quien ha centrado sus disputas y reclamos principalmente en aspectos relacionados con su estabilidad económica, por lo que la corte detalló los criterios de protección de datos personales en la legislación ecuatoriana. (Corte Constitucional del Ecuador, 2021)

Es en efecto que para aquellos años y sobre aquellos acontecimientos sociales que el Ecuador se vio en la necesidad de implementar un plan de acción, ya que en comparación de otros países de la región que llevan aplicando legislación en base a protección de datos personales, el Ecuador no contaba con uno, siendo propuesto el 19 de septiembre de 2019 por el presidente rigente de la República ante la Asamblea Nacional el Proyecto de Ley Orgánica de Protección de Datos Personales, la cual fue exitosamente aprobada y que se encuentra vigente a día de hoy.

2.2.2. COMPARACIÓN ENTRE LA LEGISLACIÓN ECUATORIANA Y EL RGPD

Para el doctor en leyes y PhD, Francisco Játiva Yánez (2023), tanto en Europa como en Ecuador, existen legislaciones específicas que regulan el tratamiento, los derechos y las obligaciones relativos a los datos personales. En el presente artículo jurídico, se llevará a cabo un análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador y la normativa europea, destacando sus similitudes y diferencias.

En primer lugar, es fundamental señalar que, tanto en Europa como en Ecuador, se reconoce el derecho fundamental de las personas a la protección de sus datos personales. En Europa, el Reglamento General de Protección de Datos (RGPD) constituye la normativa principal que regula este derecho, mientras que, en Ecuador, dicha regulación está a cargo de la Ley Orgánica de Protección de Datos Personales (LOPD).

En cuanto a las similitudes entre ambas normativas, se puede observar que tanto el RGPD como la LOPD establecen que el tratamiento de datos personales debe

realizarse de manera lícita, leal, transparente y limitada a lo necesario para los fines para los cuales se han recogido. Además, ambas normativas reconocen los derechos de acceso, rectificación, cancelación y oposición que tienen las personas sobre sus datos personales, así como el derecho a la portabilidad de los mismos (Játiva Yánez, 2023).

Respecto a las diferencias, el RGPD establece un régimen de sanciones más estricto que el de la LOPD, permitiendo multas de hasta el 4% del volumen de negocios anual mundial de la empresa infractora, mientras que en Ecuador las sanciones son más moderadas, con un régimen que considera la levedad y gravedad de ciertas acciones u omisiones.

Otra diferencia relevante es que, en Europa, su aplicación va para todas las entidades que procesan datos personales de individuos dentro de la Unión Europea, independientemente de la ubicación de la entidad.

También tiene una aplicación extraterritorial, es decir, se aplica también a organizaciones fuera de la UE si procesan datos de ciudadanos de la UE, mientras que en Ecuador se aplica a todas las entidades que procesan datos personales dentro del País e incluye disposiciones específicas para la transferencia internacional de datos personales (Diario Oficial de la Unión Europea, 2016).

Un ejemplo práctico del nivel de madurez de un ordenamiento jurídico se puede medir a través de la jurisprudencia. En el caso europeo, la sentencia del Tribunal de Justicia de la Unión Europea en el caso Schrems II es un buen ejemplo de la importancia otorgada a la protección de datos personales. En dicha sentencia, el Tribunal de Justicia anuló el acuerdo de Puerto Seguro entre la UE y los Estados Unidos debido a las deficiencias en la protección de datos personales de los ciudadanos europeos en manos de las empresas estadounidenses.

Es importante mencionar algunas consideraciones relevantes que tiene consigo la Ley Orgánica de Protección de Datos en Ecuador, en cuanto a los derechos reconocidos y garantizados, se incluye el derecho de las personas a conocer, actualizar, rectificar y eliminar los datos personales que se encuentren en cualquier base de datos o archivo que los contenga, revitalizando la figura del acceso legítimo a la información. Las personas tienen el derecho a oponerse al tratamiento de sus

datos personales cuando se realice sin su consentimiento o cuando se trate de datos sensibles (Del Pozo Basurto, 2021).

Por otra parte, en cuanto a las obligaciones, la ley establece que todas las personas, sean naturales o jurídicas, que manejen datos personales deben garantizar su protección y confidencialidad. Además, deben obtener el consentimiento explícito de las personas para el tratamiento de sus datos personales y cumplir con los principios de licitud, lealtad y transparencia en su tratamiento. Es necesario realizar esfuerzos para cumplir adecuadamente con el deber de información a cargo del responsable del manejo de estos datos y también con el deber de informarse por parte de todas las personas cuyos datos serán encargados para su tratamiento a un tercero.

Aunque el RGPD y la LOPD de Ecuador comparten muchos principios y objetivos comunes en la protección de datos personales, existen ligeras diferencias en la aplicación, la estructura regulatoria, y las sanciones debido a los contextos específicos de la UE y Ecuador.

En palabras simples, esta ley en vigencia posiciona a Ecuador en el ámbito de la protección de datos personales, destacando que reconoce el derecho fundamental de las personas a la protección de sus datos personales y establece normativas específicas para regular su tratamiento. Por ello, aunque existen similitudes con normativas internacionales e intercontinentales, se puede concluir que el ordenamiento jurídico ecuatoriano en este tema se encuentra en una etapa más que de desarrollo, es imperativo que las empresas y organizaciones que manejen datos personales estén al tanto de estas normativas y cumplan con sus obligaciones para garantizar la privacidad y seguridad de los datos de las personas.

La Ley Orgánica de Protección de Datos (LOPD) y el Reglamento General de Protección de Datos (RGPD) son dos normativas diseñadas con el propósito de garantizar la seguridad de los individuos y proteger su privacidad frente a las empresas que manejan sus datos personales. La diferencia principal entre la LOPD y el Reglamento (UE) 2016/679 radica en que la LOPD tiene un ámbito de aplicación nacional, mientras que el RGPD es una normativa de alcance europeo. No obstante, todas las empresas que necesiten tratar datos personales para el desarrollo habitual

de su actividad comercial están obligadas a cumplir con las disposiciones tanto de la LOPD como del RGPD (MICROLAB HARD S.L., 2023).

Tanto la LOPD como el RGPD tienen como objetivo la preservación de la privacidad de las personas. ¿Cómo buscan alcanzar este objetivo?, requiriendo a las empresas el diseño de estrategias y la implementación de medidas destinadas a garantizar la protección de datos personales necesarios para el desarrollo de su actividad. ¿Esto implica que las empresas no pueden manejar datos personales? no, significa que deben utilizar dichos datos de manera responsable y siempre en cumplimiento con la Ley Orgánica de Protección de Datos y el Reglamento General de Protección de Datos, normativas que protegen los datos personales de clientes, proveedores, empleados, asociados u cualquier otra figura que haya proporcionado información personal a una empresa o entidad (MICROLAB HARD S.L., 2023).

2.3. Principales aspectos del RGPD y su impacto potencial en Ecuador

El RGPD se fundamenta en varios principios que orientan el manejo de datos personales. Estos abarcan el consentimiento claro del titular de los datos, la minimización y precisión de la información, la restricción en cuanto a la finalidad del procesamiento, y la confidencialidad e integridad de los datos. Estos principios garantizan que los datos se recopilen y utilicen de manera justa, transparente y segura (LEXIS, 2023).

Para el RGPD de la Unión Europea (Diario Oficial de la Unión Europea, 2016), en su parágrafo 39, expresa que el tratamiento de datos personales debe ser lícito y leal. Las personas deben estar completamente informadas de que sus datos personales están siendo recogidos, utilizados, consultados o tratados, así como del alcance de dicho tratamiento. El conocido principio de transparencia tiene la necesidad de requerir que tanto la información y comunicación sobre el tratamiento de datos, sea fácilmente accesible y comprensible el mismo que tendrá que emplear un uso de lenguaje claro y sencillo, que será especialmente relevante para la información sobre la identidad del responsable del tratamiento y sus objetivos, así como para la información adicional que asegure un tratamiento justo y transparente para las personas involucradas, incluyendo su derecho a obtener confirmación y

acceso a sus datos personales tratados. Las personas deben estar al tanto de los riesgos, normas, salvaguardias y derechos relacionados con el tratamiento de datos personales y cómo hacer valer sus derechos. Los fines específicos del tratamiento deben ser explícitos y legítimos, determinados en el momento de la recogida de los datos. Por lo tanto, los datos personales tienen que ser apropiados, relevantes y limitados a lo estrictamente necesario para los fines del tratamiento, lo que implica limitar su conservación al mínimo necesario, los datos personales solo deben tratarse si no hay medios razonables para lograr el objetivo del tratamiento, los datos no deben conservarse más tiempo del necesario, para asegurar esto, el encargado del tratamiento debe establecer plazos para su eliminación o revisión periódica. Es fundamental tomar todas las medidas razonables para corregir o eliminar datos inexactos, los datos personales deben ser tratados de manera que se garantice su seguridad y confidencialidad, evitando el acceso o uso no autorizados de los datos y del equipo utilizado para su tratamiento.

Cabe señalar que, en 2018, Brasil aprobó su Ley General de Protección de Datos, inspirada en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Esta normativa, que entraría en vigor en 2020, incluye derechos como la portabilidad de datos, el derecho al olvido y una aplicación extraterritorial. Mientras tanto, en Ecuador, la Dirección Nacional de Registro de Datos Públicos (DINARDAP) trabajaba en un anteproyecto de ley sobre protección de datos personales. En este contexto, surgía la pregunta de si Ecuador adoptará un modelo similar al RGPD o desarrollará una normativa distinta, considerando las particularidades del país para evitar posibles problemas (Serrano, 2018).

Es importante subrayar que su impacto se viene analizando desde hace varios años tomando en cuenta datos específicos y demás contextos.

> En primer lugar, en América Latina y el Caribe viven aproximadamente 670 millones de personas distribuidas en 46 países, a partir de los años 2000, países como Argentina, Uruguay, México, Perú y Colombia desarrollaron leyes de protección de datos personales, inspiradas principalmente en la Directiva Europea 95/46/EC y en la visión europea sobre el derecho a la

privacidad. Con la entrada en vigor del RGPD en mayo de 2018, la mayoría de los países de la región reformaron o comenzaron a trabajar en normativas similares. Por ejemplo, países como Ecuador y Paraguay, que carecían de una ley específica, por aquellos años se encontraban desarrollando sus legislaciones para alinearse con este estándar, este panorama posiciono a la región como un socio estratégico para la Unión Europea en temas de protección de datos (Enríquez, 2021).

Es importante destacar que la Unión Europea se ha posicionado como uno de los principales inversionistas en América Latina y el Caribe en los últimos años, representando aproximadamente el 39% de las nuevas inversiones extranjeras directas y estableciendo cerca de 26 acuerdos de libre comercio, en este contexto, no resulta casual que los países latinoamericanos hayan adoptado el modelo europeo de protección de datos personales.

Por lo mismo cualquier organización que maneje datos de ciudadanos de la UE, sin importar dónde se encuentre, debe cumplir con esta regulación, esto ha obligado a muchas empresas en todo el mundo a ajustar sus prácticas y políticas de privacidad para alinearse con los estándares del RGPD (Reyes Amán, 2016, pág. 16).

2.3.1. DERECHOS DE LOS TITULARES DE DATOS

El RGPD concede a los ciudadanos de la UE varios derechos clave respecto a sus datos personales. Estos derechos incluyen el acceso a sus datos, la rectificación de información incorrecta, la eliminación de datos, la portabilidad de los datos y el derecho a oponerse al procesamiento. Gracias a estos derechos, los usuarios pueden controlar sus datos y determinar cómo se manejan (LEXIS , 2023).

La LOPD especifica los procedimientos que deben cumplirse para utilizar información personal, define las responsabilidades del responsable y del encargado del tratamiento de datos, y establece la creación de un órgano supervisor encargado de garantizar el cumplimiento de la ley, este órgano tiene la facultad de imponer sanciones administrativas cuando el tratamiento de datos no se ajusta a la finalidad autorizada inicialmente. Además de que la ley introduce conceptos innovadores como la figura del responsable, que puede ser una persona física o jurídica, pública o privada, con la autoridad exclusiva o conjunta para determinar la finalidad y el manejo de las bases de datos personales. Además, define al encargado como aquel que procesa estos datos en nombre y por cuenta del responsable, y establece la figura de un delegado que actúa como enlace entre el responsable y la autoridad responsable de la protección de la información. (Javier, 2022)

Del mismo modo que la ley establece que el tratamiento de datos personales requiere el consentimiento del titular, el cual debe ser libre, claro, específico e informado. Además, se subraya que este consentimiento puede ser retirado en cualquier momento, la LOPDP también regula las transferencias internacionales de datos, permitiéndolas siempre que se cumplan con todas las condiciones legales establecidas y que el país receptor garantice estándares internacionales adecuados para la protección de esos datos personales.

Según lo establecido en el Reglamento por los derechos del titular en causas de derecho por supresión (Parlamento Europeo y Consejo de la Unión Europea , 2016), en ciertas situaciones, una persona puede pedir al responsable del tratamiento que

elimine sus datos personales, como cuando los datos ya no son necesarios para el propósito para el que fueron recopilados. Sin embargo, la empresa no está obligada a hacerlo si:

- El tratamiento es necesario para proteger la libertad de expresión e información.
- Los datos personales deben conservarse para cumplir una obligación legal.
- Existen razones de interés público para mantener los datos, como en el ámbito de la salud pública o para fines de investigación científica e histórica.
- Es necesario conservar los datos personales para emprender acciones legales.

Respecto del derecho de rectificación y al derecho de oposición del RGPD (Parlamento Europeo, 2016), si por alguna razón cualquier persona considera que sus datos personales son; ya sea, incorrectos, incompletos o hasta inexactos, tiene derecho a corregirlos o actualizarlos sin demora.

En tal caso, se debe informar a todos los destinatarios de los datos personales si alguno de los datos compartidos con ellos ha sido modificado o eliminado. Si los datos personales compartidos son incorrectos, también puede ser necesario informar a todos los que los hayan consultado, a menos que esto represente un esfuerzo desproporcionado.

Nuevamente el derecho a la protección de datos surge para que los individuos puedan controlar sus propios datos, tanto en tratamientos manuales como automatizados, siendo estos últimos más peligrosos para los derechos fundamentales, la evolución de las tecnologías de la información y la comunicación ha aumentado la preocupación por proteger estos derechos en la era de Internet. Legalmente, es esencial equilibrar el desarrollo de las libertades fundamentales con el control de los datos personales. Los titulares de estos derechos suelen estar en desventaja jurídica frente a infractores con mayor conocimiento técnico y poder económico (Ordoñez, 2021).

De manera reiterada una persona también puede oponerse en cualquier momento a como se usen sus datos personales y al tratamiento de este, más aún si es para un uso en específico en el que la empresa los procesa sobre la base de un interés

legítimo o los antepone en una actividad de interés público, a no ser que prevalezca el interés de manera legítima de la empresa sobre el interés del individuo, entonces esta debe dejar de tratar los datos personales.

El objetivo del derecho a la protección de datos es asegurar que el tratamiento de la información se realice de manera adecuada, salvaguardando los derechos y libertades asociados, esto protege al titular de los datos, otorgándole el derecho a controlar su información frente al tratamiento, este control se logra mediante la atribución de derechos al titular y la imposición de obligaciones a quienes procesan los datos. Además, el habeas data permite ejercer los derechos de acceso, rectificación, cancelación y oposición (Ordoñez, 2021).

Según Ordoñez (2021), la Ley Orgánica de Protección de Datos (LOPD) de Ecuador sigue el enfoque del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, esta normativa permite a los individuos oponerse al procesamiento de sus datos personales en ciertas circunstancias: cuando no se afecten derechos de terceros, cuando lo autorice la ley, y cuando la información no sea de carácter público. Asimismo, se puede rechazar el tratamiento de datos para actividades de mercadotecnia directa o cuando no se requiera el consentimiento debido a un interés legítimo.

Sin embargo, en el caso de fines de marketing directo, la empresa siempre debe dejar de tratar los datos personales si así lo solicita el interesado. Por otro lado, en lo que se refiere al derecho de acceso y del derecho a la portabilidad de datos (Parlamento Europeo y Consejo de la Unión Europea , 2016), los ciudadanos tienen el derecho de acceder a sus datos personales de manera gratuita. Cuando se recibe una solicitud de este tipo, es necesario:

- Confirmar si se están tratando los datos personales.
- Proporcionar información sobre el tratamiento de los datos (incluyendo la finalidad, las categorías de datos personales involucrados, los destinatarios de los datos, entre otros).
- Proporcionar una copia de los datos personales en un formato accesible y sujetos a procesamiento.

De este modo si el tratamiento se fundamenta en consentimiento o contrato, la persona en cuestión que este afectada, en este caso puede pedir que le devuelvan sus datos personales además podrá pedir que los transfieran a otra empresa. Respectivamente a esto se le conoce como derecho a la portabilidad de datos, esencialmente estos últimos deben ser entregados en un formato comúnmente utilizado y legible por máquina.

2.3.2. OBLIGACIONES DE LAS EMPRESAS Y ORGANIZACIONES

Dentro del margen legal ecuatoriano, la LOPD establece por obligaciones de las empresas y organizaciones de protección de datos, en su articulado 47 que:

2.3.2.1 OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO CON LOS DATOS PERSONALES

Según la ley orgánica de protección de datos personales (2021), el responsable del tratamiento de datos personales está obligado a cumplir una serie de deberes específicos. Estos incluyen el manejo de los datos personales con estricto apego a los principios y derechos establecidos por la ley, su reglamento, y las directrices emitidas por la Autoridad (inciso 1); la implementación de medidas administrativas, técnicas, físicas, organizativas y jurídicas adecuadas para asegurar y demostrar el cumplimiento normativo (inciso 2); la realización de evaluaciones periódicas para verificar la efectividad de dichas medidas (inciso 3); y la formulación de políticas de protección de datos adaptadas a las circunstancias específicas de cada situación (inciso 4).

Dado que los datos personales pueden ser tratados incluso a nivel internacional, es esencial regular este fenómeno adecuadamente, esto se debe a la necesidad de conciliar intereses variados como la privacidad, los objetivos comerciales y la libertad de información. El principal riesgo radica en el tratamiento de datos personales, no en la existencia de los datos, por ello, es crucial un manejo

responsable de la información por parte de las entidades públicas y privadas, garantizando que el tratamiento de datos cumpla con los principios de protección establecidos (Ordoñez, 2021).

Es por eso que el tratamiento de estos datos personales debe respetar todos los principios y derechos, es decir, todo el marco legal de protección de datos, siendo esencial para garantizar la seguridad jurídica y la confianza ciudadana en la legislación de protección de datos. La falta de seguridad jurídica no solo surge de la ausencia de normas legales relacionadas con el tratamiento de información, sino también de prácticas administrativas que reducen la confianza pública en las instituciones y afectan la estabilidad en el ejercicio de derechos fundamentales y situaciones jurídicas.

Además, es esencial utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas (inciso 5); llevar a cabo evaluaciones de seguridad antes de proceder al tratamiento de datos personales (inciso 6); y adoptar medidas para prevenir, mitigar y controlar los riesgos y vulneraciones identificadas (inciso 7). También se requiere informar a la Autoridad de Protección de Datos Personales y al titular de los datos sobre cualquier incidente que afecte las medidas de seguridad implementadas (inciso 8); integrar la protección de datos personales desde la fase inicial del diseño y por defecto (inciso 9); establecer acuerdos de confidencialidad con el personal encargado del tratamiento de datos (inciso 10); y asegurar que el encargado del tratamiento ofrezca garantías adecuadas para proteger el derecho a la privacidad conforme a la normativa vigente (inciso 11).

Adicionalmente, se debe mantener actualizado el registro nacional de Protección de datos personales (inciso 12); designar a un delegado de protección de datos personales según corresponda (inciso 13); y facilitar auditorías o inspecciones por parte de auditores autorizados (inciso 14). Por último, es fundamental cumplir con todas las demás obligaciones establecidas en la ley y sus disposiciones complementarias (inciso 15) (Ley Orgánica de Protección de Datos Personales, 2021).

Por último, se recalca que el encargado del tratamiento de datos personales tendrá las mismas obligaciones que el propio responsable del tratamiento de datos personales, desde luego todo esto en la medida que sea aplicable según lo disponga la presente Ley al igual que su reglamento.

Por ello la importancia de la ley orgánica de protección de datos aprobada en mayo de 2021 deba orientarse hacia asegurar que los individuos puedan ejercer sus derechos fundamentales, incluyendo el acceso, la rectificación, la cancelación, la oposición, la limitación al tratamiento, la portabilidad y el derecho a no ser objeto de decisiones automatizadas. (Ordoñez, 2021)

Es así, que es crucial garantizar que las personas estén informadas sobre cómo se utilizan sus datos personales y tengan la capacidad de retirar su consentimiento si el tratamiento de estos datos no respeta los principios, derechos y garantías constitucionales.

2.3.3. TRANSFERENCIA INTERNACIONAL DE DATOS

De acuerdo con la revista digital jurídica Your Europe (Dirección General de Mercado Interior , 2022), cuando los datos personales se transfieran fuera de la Unión Europea, es necesario asegurar que la protección establecida por el Reglamento General de Protección de Datos (RGPD) acompañe a dichos datos. Esto significa que, si los datos se exportan a otro país, la empresa debe asegurarse de que se cumpla una de las siguientes condiciones:

1. La protección de datos en el país no perteneciente a la UE se considera adecuada.
2. La empresa asegura que se toman las medidas adecuadas para proporcionar las salvaguardias necesarias, como la inclusión de cláusulas específicas en el contrato con el destinatario no europeo de los datos personales.
3. La empresa se basa en motivos específicos (excepciones) para la transferencia, como lo viene siendo el consentimiento del interesado.

Así mismo para la transferencia de datos personales, de acuerdo con la Ley Orgánica de Protección de Datos Personales en Ecuador (Asamblea Nacional,

2021), las empresas deberán de seguir lo siguiente, contemplado con los artículos 55 al 59 del mismo cuerpo normativo:

La transferencia o comunicación internacional de datos personales. Tendrá factibilidad solo si se ajusta a lo estipulado en el presente capítulo, la presente Ley o la normativa especializada en la materia, asegurando siempre así el ejercicio efectivo del derecho a la protección de datos personales.

Transferencia o comunicación internacional de datos personales a países con nivel adecuado de protección. Como principio general, la transferencia o comunicación de datos personales se podrá realizar desde organizaciones, países, así como personas jurídicas que ofrezcan niveles adecuados de protección y que cumplan con la obligación de garantizar estándares reconocidos internacionalmente según los criterios establecidos en el Reglamento de la Ley.

La Autoridad de Protección de Datos Personales tiene la capacidad de implementar métodos de control ex post cuando la naturaleza de la transferencia de datos lo requiera, según el Reglamento de la Ley. Además, coordinará acciones conjuntas con las autoridades de los países involucrados para prevenir y corregir el tratamiento indebido de datos. Para asegurar que la transferencia internacional de datos cumple con los niveles adecuados de protección, emitirá una resolución motivada conforme a la ley y su reglamento (Ley de Protección de Datos Personales, 2021).

Transferencia o comunicación mediante garantías adecuadas. Si una transferencia internacional de datos se realiza hacia un país, organización o territorio económico que no ha sido calificado por la Autoridad de Protección de Datos como poseedor de un nivel adecuado de protección, la transferencia puede llevarse a cabo siempre y cuando el responsable o encargado del tratamiento de los datos personales proporcione garantías adecuadas para el titular de los datos. Estas garantías deben incluir: (a) asegurar que los principios, derechos y obligaciones en el tratamiento de datos personales se cumplan según un estándar igual o superior al de la normativa ecuatoriana vigente; (b) ofrecer una tutela efectiva del derecho a la protección de datos personales, mediante la disponibilidad continua de recursos

administrativos o judiciales; y (c) el derecho a solicitar una reparación integral cuando sea necesario (Ley de Protección de Datos Personales, 2021).

Para asegurar esto, la transferencia internacional de datos personales se basará en un marco legal que no solo cumpla con los estándares mencionados previamente, sino que también se alinee con las directrices establecidas por la Autoridad de Protección de Datos Personales. Este marco legal debe ser vinculante y garantizar que los datos sensibles de los individuos se manejen con los más altos niveles de seguridad y confidencialidad.

Es crucial que cualquier instrumento jurídico utilizado para la transferencia de datos respete plenamente los derechos de privacidad de los individuos y cumpla con las regulaciones vigentes. Esto incluye la implementación de medidas técnicas y organizativas adecuadas para proteger la información personal contra accesos no autorizados, pérdidas o modificaciones indebidas.

Normas corporativas vinculantes. De acuerdo con la ley, los responsables o encargados del tratamiento de datos personales pueden proponer normas corporativas vinculantes específicas a su actividad para la aprobación de la Autoridad de Protección de Datos Personales. Estas normas deben cumplir con ciertos requisitos: deben ser obligatorias para el responsable del tratamiento y cualquier empresa que reciba los datos; proporcionar a los titulares de los datos mecanismos adecuados para ejercer sus derechos según la ley; incluir un listado detallado de empresas afiliadas que forman parte del mismo grupo empresarial, incluyendo su estructura y datos de contacto; detallar las empresas que manejarán los datos personales, las categorías de datos y los tipos de tratamientos que se realizarán; cumplir con todos los principios y medidas de seguridad estipulados en la ley; aceptar la responsabilidad por cualquier violación de estas normas, a menos que se demuestre que no son culpables de la violación; proporcionar información clara y completa sobre las normas; designar a delegados de protección de datos y otros supervisores para asegurar el cumplimiento de las normas; establecer mecanismos detallados para que los titulares verifiquen el cumplimiento de las normas, incluyendo auditorías de protección de datos y métodos para acciones correctivas; coordinar con la Autoridad de Protección de Datos Personales; y

comprometerse a promover la protección de datos personales entre sus empleados mediante formación continua. La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos relacionados con estas normas (Ley de Protección de Datos Personales, 2021).

Autorización para transferencia internacional. Para las transferencias internacionales de datos personales que no estén cubiertas por los artículos anteriores, es necesario obtener autorización de la autoridad de protección de datos. Esta autorización requiere la demostración documentada de que se cumplen todas las normativas vigentes sobre protección de datos personales, de acuerdo con lo especificado en el reglamento correspondiente. Además, cualquier transferencia internacional de datos personales debe ser registrada previamente en el registro nacional de protección de datos personales por el responsable o encargado del tratamiento, siguiendo el procedimiento establecido en el reglamento aplicable en cuestión (Ley de Protección de Datos Personales, 2021).

2.3.4 CONSECUENCIAS DE INCUMPLIMIENTO Y SANCIONES

El incumplimiento del Reglamento General de Protección de Datos (RGPD) puede conllevar sanciones severas, incluyendo multas de hasta 20 millones de euros o el 4% del volumen de negocios global de la empresa, según la gravedad de la infracción. Además, la autoridad de protección de datos tiene la facultad de imponer medidas correctivas adicionales, como la orden de cesar el tratamiento de los datos personales (Dirección General de Mercado Interior , 2022).

Infracciones Leves

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece en su artículo 67 las sanciones para las faltas leves aplicables al "responsable" y en su artículo 69 las aplicables al "encargado" de protección de datos. En contraste, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) de España define en su artículo 74 las sanciones para faltas leves que se aplican tanto al responsable como al encargado.

Infracciones Graves

Para las faltas graves, la LOPDP de Ecuador especifica en el artículo 68 las sanciones para el "responsable" y en el artículo 70 para el "encargado" de protección de datos. En comparación, la LOPDGDD de España establece en su artículo 73 las sanciones para faltas graves aplicables tanto al responsable como al encargado.

Infracciones muy graves

En cuanto a las faltas muy graves, la LOPDP de Ecuador no define un artículo específico, mientras que la LOPDGDD de España lo hace en su artículo 72, aplicable tanto al responsable como al encargado. Adicionalmente, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece el régimen sancionador en su artículo 83, apartados 4, 5 y 6, utilizando las disposiciones del artículo 58.2, literales a) a h) y j).

De igual forma como el tipo de infracciones, las multas se dividen en tres categorías:

Multas Leves: Para las reglamentaciones del RGPD de la Unión Europea, no son especificados dentro del Reglamento, mientras que, en el LOPD en Ecuador, las multas leves van desde 1 a 10 salarios básicos unificados del trabajador en general (SBU) o del 0.1% a los 0.7% dependiendo del volumen del negocio.

Multas Graves: Para la normativa del RGPD la multas en este nivel van desde los 10 millones de euros, o del pago del 2% de la factura de la totalidad del año. Por otro lado, la LOPD ecuatoriana ronda entre los 10 a 20 SBU o del 0.7%al 1% del volumen del negocio.

Multas Muy graves: El RGPD multa con 20 millones de euros o del pago del 4%de la factura por año, en cambio, la LOPD en Ecuador no son establecidas para este nivel.

Las multas en España son superiores en comparación con Ecuador tanto para las faltas leves como para las graves, con la excepción de las infracciones muy graves, ya que en el país latinoamericano aún no se ha establecido el valor de la sanción correspondiente (Grupo Atico34, 2022).

Aunque las sanciones económicas en Ecuador no son tan severas como las establecidas en la Unión Europea, considerando el volumen económico empresarial que es significativamente mayor en la UE, las sanciones definidas en el artículo 73 de la LOPDP están relacionadas con el margen de ventas (Ruiz M., 2021).

En contraste, aunque las sanciones definidas en el artículo 73 de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador pueden parecer menos severas en términos absolutos, su relación con el margen de ventas sugiere un enfoque proporcional a la escala económica local. Este método busca adaptar las sanciones a la realidad económica del país, permitiendo que las multas sean lo suficientemente disuasorias sin ser excesivamente punitivas para las empresas ecuatorianas, las cuales operan en un mercado más pequeño y menos desarrollado en comparación con la Unión Europea.

2.4. ANÁLISIS DEL IMPACTO DEL RGPD EN LAS POLÍTICAS DE PROTECCIÓN DE DATOS EN ECUADOR

El RGPD ha tenido un impacto profundo en Ecuador, no solo influenciando la legislación a través de la Ley Orgánica de Protección de datos, sino también promoviendo una cultura de la misma, más templada y consciente. Del mismo modo que ha destacado la importancia de tener una autoridad independiente para supervisar el cumplimiento de las leyes de protección de datos. Inspirado en esto, Ecuador ha establecido su propia autoridad de protección de datos para garantizar la supervisión y aplicación efectiva de la LOPD.

Según la LOPDP, en el artículo 10, apartado k, referente a los principios fundamentales de la ley, se establece que para proteger de manera efectiva los derechos y libertades de los titulares de datos, los responsables deben ser capaces de demostrar la implementación de medidas de protección de datos personales, esto implica no solo cumplir con lo establecido explícitamente en la ley, sino también adoptar estándares, prácticas óptimas, esquemas de autorregulación, códigos de conducta en materia de protección, sistemas de certificación, etiquetas de protección de datos personales u otros mecanismos considerados adecuados

según los objetivos, la naturaleza de los datos personales o el riesgo asociado al tratamiento. (Guerra & Navarrete, 2023)

La práctica de realizar evaluaciones de impacto sobre la protección de datos para actividades de procesamiento de alto riesgo, como se exige en el RGPD, ha sido incorporada en la normativa ecuatoriana. Esto promueve una cultura de responsabilidad proactiva y gestión de riesgos dentro de las organizaciones que manejan datos personales.

Para que una empresa inicie operaciones basadas en datos, es necesario atravesar una transformación. Este proceso comienza con la identificación de soluciones de negocio, que posteriormente conducen a la creación de motores de datos y algoritmos que permiten a la organización tomar decisiones fundamentadas en datos.

En este contexto, dando un vistazo, los datos personales del área de la salud son especialmente sensibles, pues abarcan aspectos como el estado de salud, características físicas y vida sexual de una persona. Por tanto, su tratamiento debe ser realizado únicamente con el consentimiento previo, expreso y escrito del titular de los derechos, respetando siempre los principios de confidencialidad y secreto profesional.

El consentimiento previo y explícito puede ser omitido solo para proteger los intereses vitales de la persona, en situaciones donde esta no esté en capacidad física o jurídica de proporcionarlo. También se puede omitir cuando es necesario para medicina preventiva, diagnósticos médicos, tratamientos o gestión de sistemas de salud. En estos casos, es esencial asegurar la anonimización o pseudoanonimización de los datos para evitar la identificación de las personas (Grupo Bravco S.A., 2023).

Asimismo, todo tratamiento de datos de salud debe ser autorizado por la Autoridad de Protección de Datos Personales. Por lo tanto, para utilizar los datos de sus usuarios y pacientes, los prestadores de servicios de salud, profesionales del sector, y cualquier entidad que maneje este tipo de datos, como los laboratorios farmacéuticos con acceso a datos de recetas médicas deben obtener el

consentimiento previo y escrito, anonimizar los datos y obtener autorización expresa de la Autoridad de Protección de Datos Personales.

Las empresas en Ecuador, especialmente aquellas con relaciones comerciales internacionales, han tenido que adaptar sus políticas y prácticas de protección de datos para cumplir con los estándares similares al RGPD. Esto ha llevado a una revisión y fortalecimiento de las políticas de privacidad tanto en el sector privado como en el público.

La implementación del Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales ha generado un cambio considerable en la regulación de la protección de datos personales para las empresas.

Los principales cambios incluyen la obligación de nombrar un delegado de protección de datos, redactar e implementar cláusulas informativas adecuadas para los interesados, formalizar contratos para regular el acceso a datos por parte de proveedores, registrar actividades de tratamiento, realizar análisis de riesgos y evaluaciones de impacto, y garantizar la seguridad de los datos personales (Grupo Bravco S.A., 2023).

El incumplimiento en esta materia puede acarrear, además de daños reputacionales, sanciones económicas considerables. En el sector turístico, en plena expansión tecnológica, es esencial incluir elementos técnicos, legales y corporativos para garantizar la identidad digital del usuario. Planificar viajes completamente desde plataformas electrónicas y aplicaciones es conveniente, pero también conlleva riesgos significativos: ¿dónde se están dejando los datos y qué se está haciendo con ellos?

Nombre completo, edad, número de pasaporte, correo electrónico, teléfono, tarjeta de crédito o débito, la lista de datos que se debe proporcionar incluye casi toda la clasificación de información sensible. Esto representa una gran responsabilidad para las empresas que los reciben y un riesgo considerable para los usuarios. Si un hacker roba esta información o si un empleado interno hace un mal uso de ella, puede haber graves consecuencias para la empresa turística, desde multas hasta demandas, dañando su prestigio, uno de sus activos más valiosos (Grupo Bravco S.A., 2023).

Agencias de viajes, hoteles, plataformas online para reservas de vuelos o paquetes turísticos, servicios de guías o establecimientos de ocio y turismo rural son solo algunos ejemplos de empresas que necesitan operar con datos personales de los clientes y usuarios de sus servicios. Las empresas en Ecuador, especialmente aquellas con relaciones comerciales internacionales, han tenido que adaptar sus políticas y prácticas de protección de datos para cumplir con los estándares similares al RGPD. Esto ha llevado a una revisión y fortalecimiento de las políticas de privacidad tanto en el sector privado como en el público, todas ellas deben invertir en sistemas de seguridad esenciales para proteger este volumen de datos e información.

2.4.1 APLICACIÓN DEL REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCION DE DATOS PERSONALES

El Reglamento de la Ley Orgánica de Protección de Datos Personales publicado en el año 2023, ha supuesto un avance exponencial para el país a la hora de desarrollar la normativa correspondiente para la aplicación de la LOPDP. Esto último impulsado por la necesidad de establecer con claridad los preceptos y procedimientos para la ejecución de la Ley. (Reglamento de la Ley Organica de Proteccion de Datos, 2023). La aplicación del Reglamento de la Ley Orgánica de Protección de Datos Personales en Ecuador es esencia, establecer un marco normativo que orienta a los responsables del tratamiento en la implementación de medidas y procedimientos que aseguren la protección de los datos personales.

El Reglamento se aplica a todas las personas, tanto naturales como jurídicas, de cualquier nacionalidad, ya sea del sector público o privado, que manejen datos personales, independientemente de si sus actividades se desarrollan dentro o fuera de Ecuador. Asimismo, se aplica al tratamiento de datos personales de individuos no residentes en Ecuador, siempre que dichas actividades se realicen en el territorio ecuatoriano. Además, abarca a los responsables y encargados de tratamiento de datos personales no establecidos en Ecuador, quienes, por estar sujetos a la legislación nacional en virtud de un contrato o normativas internacionales, deberán

designar a un apoderado especial conforme al artículo 3 del Reglamento (Reglamento de la Ley Orgánica de Protección de Datos Personales, 2023).

Uno de los aspectos más importantes del reglamento es la evaluación de impacto del tratamiento de datos personales (art. 29), la cual requiere que los responsables realicen un análisis preventivo para identificar y mitigar posibles riesgos antes de proceder con el tratamiento de datos. Este proceso no solo es un requisito técnico, sino también una obligación ética para garantizar que los derechos de los titulares no se vean comprometidos durante el manejo de su información personal. (Reglamento de la Ley Orgánica de Protección de Datos Personales, 2023).

En cuanto a las obligaciones de los responsables y encargados del tratamiento de datos, el artículo 33 señala que el responsable del tratamiento de datos personales debe implementar medidas adecuadas durante la selección de los métodos de tratamiento y el procesamiento de los datos, para asegurar el cumplimiento efectivo de los principios de protección de datos y los derechos establecidos por la ley. Estas medidas deben considerar factores como el estado de la tecnología, los costos de aplicación, la naturaleza y el alcance del tratamiento, así como los posibles riesgos para los intereses de los titulares (Reglamento de la Ley Orgánica de Protección de Datos Personales, 2023).

El reglamento enfatiza la necesidad de implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales. También se establece la obligación de notificar cualquier brecha de seguridad que pueda comprometer la información, tanto a la autoridad de control como, en algunos casos, a los titulares de los datos. Asimismo, el reglamento introduce la obligación de realizar evaluaciones de impacto en la protección de datos antes de llevar a cabo actividades de tratamiento que puedan representar un alto riesgo para los derechos de los titulares.

Para determinar si un país, organización o persona jurídica cuenta con un nivel adecuado de protección de datos, se deben considerar varios criterios. Estos incluyen la legislación nacional y sectorial relacionada con la protección de datos, así como la normativa de seguridad nacional y pública, con especial atención a las disposiciones que permiten el acceso a datos personales por parte de las

autoridades. También se debe evaluar la normativa sobre transferencias de datos a terceros, la jurisprudencia en protección de datos, el reconocimiento de derechos y los mecanismos para ejercerlos, las obligaciones de los responsables del tratamiento de datos, y la existencia de una autoridad independiente que supervise y sancione el cumplimiento de la normativa. Además, se tomarán en cuenta los compromisos internacionales en materia de protección de datos personales (Reglamento de la Ley Orgánica de Protección de Datos Personales, 2023, art. 73). Respecto a la transferencia internacional de datos, el reglamento impone restricciones, permitiendo que estos movimientos se realicen únicamente hacia países que ofrezcan un nivel adecuado de protección de datos, o bajo condiciones específicas que garanticen la seguridad y confidencialidad de la información.

Finalmente, el articulo 90 del reglamento detalla un régimen sancionador para aquellos que incumplan las disposiciones de la ley y sus normas complementarias, iniciando el correspondiente procedimiento administrativo sancionatorio, de conformidad con las disposiciones establecidas en el Código Orgánico Administrativo. (Reglamento de la Ley Orgánica de Protección de Datos Personales, 2023).

2.4.2. EVALUACIÓN DE LA ADECUACIÓN DE LAS POLÍTICAS DE PROTECCIÓN DE DATOS ECUATORIANAS AL RGPD

La evaluación de la adecuación de las políticas de protección de datos ecuatorianas al Reglamento General de Protección de Datos (RGPD) europeo revela varias áreas clave en las que el marco legal ecuatoriano puede mejorarse. El RGPD es considerado uno de los estándares más estrictos y completos en términos de protección de datos personales a nivel global. Este reglamento otorga a los ciudadanos de la UE derechos significativos sobre sus datos personales y establece fuertes obligaciones para las empresas que manejan dicha información.

Por su parte en la Constitución de la República del Ecuador se reconoce el derecho a la protección de datos personales, con el objetivo de asegurar la seguridad jurídica de los ciudadanos, se establecen diversas garantías para los derechos personales,

como el acceso libre a la información generada por entidades públicas y por aquellas entidades privadas que manejen fondos estatales o desempeñen funciones públicas. Aparte esto asegura que los ciudadanos no enfrenten restricciones de acceso a la información, salvo en los casos claramente definidos por la ley, la misma constitución también aborda el derecho a la portabilidad de datos, asegurando la confidencialidad de la información personal almacenada en archivos de instituciones ecuatorianas en el extranjero. Del mismo modo que se asegura el derecho a la protección de datos personales, lo cual incluye el acceso y la capacidad de decisión sobre el uso de esta información.

Según un informe de Garrigues (2018), varias naciones en Latinoamérica, incluyendo Ecuador, están adoptando elementos del RGPD para reforzar sus propias leyes de protección de datos, este proceso de adecuación es crucial para asegurar que las políticas locales sean robustas y alineadas con las mejores prácticas internacionales. Además, se destaca la necesidad de adaptar las normativas nacionales para garantizar una adecuada protección y control de los datos personales, permitiendo a los titulares de los datos ejercer sus derechos de manera efectiva.

Al adoptar estos estándares, las empresas pueden mejorar su reputación, evitar sanciones significativas y fomentar un entorno de innovación tecnológica segura, la protección adecuada de los datos personales es un componente esencial para la modernización y digitalización de los servicios en la región, siendo más segura y confiable, promoviendo un mayor respeto por la privacidad y los derechos de los ciudadanos.

Por ello es obligatorio llevar a cabo una evaluación de impacto sobre la protección de datos cuando el tratamiento previsto pueda representar un alto riesgo para los derechos y libertades de las personas, como cuando se utilizan nuevas tecnologías (Dirección General de Mercado Interior , 2022).

- Se considera que existe un alto riesgo en los siguientes casos:
- Se utiliza el tratamiento automatizado y la elaboración de perfiles para evaluar a las personas.

- Se observa una zona de acceso público a gran escala (por ejemplo, mediante circuito cerrado de televisión).
- Se tratan a gran escala categorías especiales de datos (por ejemplo, datos de salud) o datos personales relacionados con condenas e infracciones penales.
- Nota: las autoridades de protección de datos pueden identificar otras categorías de tratamiento de datos como de alto riesgo.

Si las medidas propuestas en la evaluación de impacto sobre la protección de datos no eliminan todos los altos riesgos identificados, se debe consultar a la autoridad de protección de datos antes de proceder con el tratamiento. La automatización de la información presenta aspectos positivos y negativos, aunque el uso del internet y las transacciones electrónicas han facilitado avances significativos en las administraciones actuales, también han provocado filtraciones y divulgan errónea de información que en ocasiones han vulnerado los derechos de las personas afectadas. El inminente avance y acceso masivo a datos personales por parte de las nuevas tecnologías representa una amenaza potencial para las libertades y derechos consagrados en la Constitución, esto es especialmente preocupante cuando se trata de información sensible, que debe ser gestionada adecuadamente para evitar la vulneración de los derechos constitucionales de los individuos. (Chicaiza Mullo, 2023)

Al adoptar estos estándares, las empresas pueden mejorar su reputación, evitar sanciones significativas y fomentar un entorno de innovación tecnológica segura, la protección adecuada de los datos personales es un componente esencial para la modernización y digitalización de los servicios en la región.

2.4.3. IMPACTO EN EMPRESAS Y ORGANIZACIONES ECUATORIANAS

El RGPD ha tenido un impacto considerable y significativo en el país el cual se ve reflejado de conformidad con lo dispuesto en la Ley Orgánica de Protección de Datos Personales vigente en la República del Ecuador, haciendo que las empresas y organizaciones ecuatorianas trabajen en concordancia con este último, obligándolas a revisar y fortalecer sus políticas de privacidad, designar

responsables de protección de datos, realizar evaluaciones de impacto, y adoptar nuevas tecnologías de seguridad.

La normativa, vigente es aplicable a todas las entidades públicas y privadas. Marco Rodríguez, presidente de la Asociación de Bancos Privados del Ecuador (Asobanca), indico en 2023 que el sistema financiero comenzó a adaptar sus políticas y controles al nuevo marco legal desde la promulgación de la Ley Orgánica de Protección de Datos Personales. Según Rodríguez, los bancos están revisando cada contrato de productos y servicios financieros suscritos con sus clientes para añadir o modificar cláusulas, en conformidad con las nuevas disposiciones legales y en beneficio de los derechos de sus clientes (González, 2023).

Las palabras del señor Marco Rodríguez no se quedaron ahí, pues dentro del ámbito de aplicación de su política y de conformidad con lo dispuesto en la Ley Orgánica de Protección de Datos Personales. La Asociación de Bancos Privados del Ecuador (ASOBANCA) se encargará de gestionar los datos personales proporcionados de manera legítima y legal por los titulares, incluyendo información como nombres, direcciones, números de cédula, fechas de nacimiento, y datos de contacto (ASOBANCA, 2023.).

Dentro de este proceso de adaptación a la Ley también se encuentran los hospitales y clínicas. Al igual que en el caso de los bancos, este sector tiene experiencia en la gestión de datos personales. Alejandra García, asesora legal del Hospital Alcívar en Guayaquil, menciona que el sector sanitario ya cumplía con normativas relacionadas con la confidencialidad de los datos y el historial clínico de los pacientes. Con la nueva Ley de Protección de Datos Personales, se ha añadido el concepto de "datos personales sensibles", regulando el secreto profesional de una manera diferente y abordando también las brechas de seguridad informática. Entre las medidas adoptadas por el Hospital Alcívar está la actualización de su reglamento general, que ahora incluye la creación de un Comité de Protección de Datos encargado de proteger los datos sensibles. Además, el hospital está capacitando a su personal, y García, quien está cursando un Máster en Protección de Datos en la Universidad de La Rioja, ofrece conferencias sobre el tema. En el sector público, la Dirección Nacional de Registros Públicos emitió en junio de 2021 la resolución 009

para regular el tratamiento de datos personales en las instituciones públicas. La guía cuenta con seis anexos que cubren aspectos como la recopilación de datos personales, el propósito de dicha recolección, un plan de acción para mitigar amenazas y un modelo de acuerdo de confidencialidad. Angie Jijón, directora nacional de Registros Públicos, destaca que han implementado medidas legales y tecnológicas para asegurar la protección de los datos personales, además de trabajar en ciberseguridad. Jijón también menciona que realizan controles a las entidades públicas para evaluar el progreso del plan de cumplimiento e implementación de la normativa (González, 2023).

2.4.4. PERCEPCIÓN Y CUMPLIMIENTO DEL RGPD POR PARTE DE LAS EMPRESAS ECUATORIANAS

Las empresas deben evidenciar su conformidad con el Reglamento General de Protección de Datos (RGPD) y cumplir con todas las obligaciones pertinentes, particularmente cuando lo requiera la autoridad de protección de datos o durante una inspección. Para lograr esto, es esencial mantener registros detallados que incluyan información como: el nombre y los datos de contacto de la empresa involucrada en el tratamiento de datos, los motivos para dicho tratamiento, una descripción de las categorías de individuos cuyos datos se recopilan, las categorías de organizaciones que reciben estos datos, cualquier transferencia de datos personales a otro país u organización, el período durante el cual se almacenarán los datos, y una descripción de las medidas de seguridad implementadas en el tratamiento de los datos. Además, la empresa debe mantener y actualizar regularmente las directrices y procedimientos escritos, asegurándose de comunicarlos a sus empleados (Parlamento Europeo, 2016). Además, la empresa debe mantener y actualizar periódicamente las directrices y procedimientos escritos, y comunicarlos a sus empleados.

Para asegurar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD) en Ecuador, las empresas pueden seguir estos pasos:

- Concientización: Capacitar a su personal sobre las disposiciones de la ley y la importancia de la protección de datos.
- Registro de Actividades de Tratamiento: Mantener un registro detallado de todas las actividades de procesamiento de datos personales.
- Política de Privacidad: Elaborar y publicar una política de privacidad clara y accesible que explique cómo se recopilan, almacenan y utilizan los datos personales.
- Seguridad de Datos: Implementar medidas de seguridad robustas para proteger los datos personales contra el acceso no autorizado.
- Consentimiento: Obtener el consentimiento informado y explícito antes de recopilar y procesar datos personales.
- Derechos de las Personas: Establecer procedimientos internos para garantizar que las personas puedan ejercer sus derechos sobre sus datos personales.
- Notificación de Brechas: Tener un plan de respuesta a incidentes que incluya la notificación adecuada en caso de una violación de seguridad.

La Ley de Protección de Datos en Ecuador es una medida crucial para garantizar la privacidad y la seguridad de los datos personales de los ciudadanos ecuatorianos. Las empresas que operan en el país deben tomar en serio su cumplimiento y adherirse a las mejores prácticas en la gestión de datos personales (Blog Gobierno Corporativo, 2023).

Su objetivo de salvaguardar la privacidad y seguridad de la información personal de los ciudadanos constituye una medida fundamental en el panorama jurídico y tecnológico del país, esta legislación se enfoca en establecer un marco regulatorio claro y preciso que obliga a las empresas y organizaciones, tanto nacionales como extranjeras, a adoptar y mantener altos estándares en la recolección, almacenamiento, procesamiento y transferencia de datos personales.

Como se ve, la importancia de esta ley radica en varios aspectos, en primer lugar, consolida que las personas ecuatorianas tengan un gran control de su información personal permitiéndoles conocer qué datos se recopilan y cómo se utilizan, a la vez con quién se comparten.

Para las empresas que operan en Ecuador, el cumplimiento de esta normativa no es solo una obligación legal, sino también una oportunidad para fortalecer la confianza de sus clientes y mejorar su reputación en el mercado. Las compañías deben implementar políticas de privacidad transparentes y procedimientos robustos para la gestión de datos, asegurando que la información personal esté protegida contra accesos no autorizados, pérdida, divulgación y cualquier forma de tratamiento ilícito.

Cumplir con las normativas de protección de datos no solo es una obligación legal, sino que también ofrece varios beneficios para las empresas, al proteger adecuadamente los datos personales, las empresas pueden fortalecer la confianza de sus clientes, lo que puede traducirse en una mayor lealtad y satisfacción.

El cumplimiento normativo reduce el riesgo de sanciones y multas, que pueden ser significativas en caso de incumplimiento del RGPD o la LOPD Además, las empresas que demuestran un fuerte compromiso con la protección de datos pueden diferenciarse en el mercado, atrayendo clientes que valoran la privacidad y la seguridad de su información personal y finalmente, adoptar altos estándares de protección de datos puede fomentar la innovación dentro de la empresa, promoviendo la creación de soluciones seguras y respetuosas con la privacidad.

CONCLUSIONES

La evolución del marco normativo de protección de datos en Ecuador ha estado influenciada por tendencias y estándares internacionales, entre ellos el RGPD de la Unión Europea. Sin embargo, el desarrollo normativo ecuatoriano ha seguido su propio proceso, adoptando principios que reflejan las mejores prácticas en la regulación de la protección de datos.

Uno de los principales desafíos ha sido que las organizaciones deben realizar inversiones significativas en infraestructura tecnológica para cumplir con los requisitos de protección de datos, como la implementación de medidas de seguridad y la realización de evaluaciones de impacto. Este proceso puede ser costoso y complejo, especialmente para pequeñas y medianas empresas.

La implementación de estándares similares al RGPD ha demando un nivel alto de conocimiento y conciencia sobre la protección de datos tanto en el sector público como en el privado, esto ha creado la necesidad de capacitar a funcionarios, empresas y ciudadanos sobre sus responsabilidades y derechos en materia de protección de datos. Entre las oportunidades, la adaptación al RGPD ha permitido a Ecuador modernizar su marco legal y regulatorio, alineándolo con las mejores prácticas internacionales, no solo mejorando la protección de datos, sino que también ha contribuido a una gobernanza más efectiva en el ámbito digital. Por otra parte, al alinearse con el RGPD, Ecuador ha facilitado el comercio y la cooperación internacional, del mismo modo que ha fomentado la transparencia en el tratamiento de datos personales y el desarrollo de nuevas competencias.

El alto estándar que prevé el RGPD impactó en modificaciones legislativas y regulatorias, como la publicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2021 que adaptó el marco regulador ecuatoriano a las exigencias minimas del RGPD. La LOPDP estableció un enfoque que sigue principios similares a los del RGPD, como el consentimiento explícito y la transparencia en el tratamiento de datos. La ley también reconoce y protege los derechos de los titulares de datos, incluyendo los derechos de acceso, rectificación, cancelación y oposición, en línea con el RGPD. Se elaboró ademas el Reglamento

de la Ley Orgánica de Protección de Datos Personales, que proporciona directrices más detalladas sobre la implementación de la ley. Este reglamento establece procedimientos específicos para la realización de evaluaciones de impacto sobre la protección de datos, exige la adopción de medidas de seguridad adecuadas y regula las condiciones bajo las cuales se pueden realizar transferencias internacionales de datos. Además, el reglamento define la estructura y las competencias de la Superintendencia de Protección de Datos Personales, que actúa como la autoridad reguladora encargada de supervisar y garantizar el cumplimiento de la normativa. La LOPDP y su reglamento establecen criterios rigurosos para asegurar que los datos personales transferidos a otros países cuenten con un nivel adecuado de protección, similar a los requisitos del RGPD. Esto ha llevado a Ecuador a adoptar un enfoque más estricto en la regulación de las transferencias internacionales, garantizando que las prácticas de protección de datos estén alineadas con los estándares globales.

El RGPD ha influído en la forma en que las organizaciones ecuatorianas tratan datos pues en nuestra legislación tambien se determina la obligación de realizar evaluaciones de impacto sobre la protección de datos es una de las influencias clave del RGPD, esto implica realizar análisis previos para identificar posibles riesgos para la privacidad y establecer medidas para reducir estos riesgos antes de llevar a cabo actividades de tratamiento que puedan afectar a los derechos de los titulares. Esto ha llevado a un mayor escrutinio de las transferencias internacionales y a la adopción de cláusulas contractuales estándar y otros mecanismos para garantizar un nivel adecuado de protección de datos en países terceros.

Teniendo en cuenta que en razón de que el RGPD determina que es aplicable incluso a las empresa establecidas fuera de la UE que ofrecen productos o servicios, gratuitos u onerosos a ciudadanos de la UE como es el caso de algunas empresas ecuatorianas, ha tenido un impacto significativo en la forma en que las organizaciones ecuatorianas tratan la información personal, promoviendo una mayor rigidez en las políticas de protección de datos, la implementación de medidas de seguridad adecuadas, la realización de evaluaciones de impacto, y el fortalecimiento de los derechos de los titulares de datos, reflejando así un esfuerzo

por mejorar la protección de datos personales y garantizar el cumplimiento de estándares internacionales en un entorno globalizado.

RECOMENDACIONES

El proveer de más recursos y facultades a la autoridad de protección de datos en Ecuador para que pueda supervisar y hacer cumplir efectivamente la legislación, incluyendo la capacidad de imponer sanciones significativas en caso de incumplimiento.

Otro punto importante que mencionar, para que Ecuador este mejor posicionado con los estándares internacionales, deberá promover la cooperación y el intercambio de información con otros entes internacionales y también con otros países que hallan implementado normativas firmes en lo que respecta a protección de datos como el RGPD en la Unión Europea, suponiendo así una cooperación que no solo facilitaría el comercio y la colaboración entre fronteras, sino que a la par contribuiría al desarrollo de un mecanismo digital global más seguro.

Es crucial mantener el fortalecimiento de los derechos individuales de los ciudadanos ecuatorianos en términos de control sobre sus datos personales. Establecer requisitos claros para la seguridad de los datos personales, incluyendo políticas de gestión de riesgos, auditorías periódicas y planes de respuesta ante incidentes, esto ayudaría a fomentar la adopción de estándares de seguridad reconocidos internacionalmente para proteger la información sensible, el promover la transparencia y responsabilidad en las prácticas de recopilación, uso y almacenamiento de datos personales es otro aspecto clave.

Por supuesto las organizaciones ecuatorianas también deben ser más transparentes en sus prácticas de manejo de datos, implementando mecanismos efectivos de rendición de cuentas y sanciones proporcionales para aquellos que no cumplan con las regulaciones de protección de datos.

Del mismo modo, la optimización de las transferencias internacionales de datos desde y hacia Ecuador bajo estándares internacionales de privacidad también resulta esencial, el desarrollar políticas y procedimientos claros para asegurar que las transferencias de datos cumplan con estándares adecuados de protección, y garantizar que el mismo cumpla con estos estándares, contribuyendo significativamente a fortalecer la protección de datos en el país.

La educación y concienciación también son claves. Se deben implementar campañas de sensibilización pública sobre la importancia de la protección de datos y los derechos de los ciudadanos, así como fomentar la formación en protección de datos dentro de las organizaciones para asegurar que el personal maneje correctamente la información personal.

Si bien la implementación de estas recomendaciones representa desafíos significativos, como costos asociados y la necesidad de capacitación y recursos adecuados, los beneficios potenciales son considerablemente altos. Alinear el marco legal de protección de datos de Ecuador con el RGPD no solo mejorará la protección de la privacidad de los individuos y la seguridad de la información, sino que también fortalecerá la confianza del consumidor, promoverá la innovación y el desarrollo tecnológico responsable, y facilitará el acceso a mercados internacionales.

Nuevamente el cambio cultural es otro desafío, ya que cambiar la mentalidad organizacional para priorizar la protección de datos puede ser un proceso lento y difícil, además por lo cual será necesario implementar programas continuos de educación y concienciación tanto para el público en general como para los empleados de las organizaciones.

Si lo vemos desde una perspectiva social y política, la protección de los datos personales fortalecería la democracia y los derechos humanos lo que iría en concordancia con nuestra carta magna, asegurando que los datos se manejen con respeto a la privacidad y la autonomía de los individuos, además, una mayor transparencia en el uso de datos por parte del gobierno y las empresas fortalecería la confianza entre las instituciones.

Visto de otro modo, en términos de competitividad económica, nuestro país se volvería más atractivo para las inversiones, ya que las empresas internacionales y locales estarían más dispuestas a invertir en un entorno donde las leyes de protección de datos son claras y estrictas, minimizando riesgos legales. Además de por supuesto, cumplir con los estándares internacionales lo que facilitaría a las empresas ecuatorianas operar en mercados globales.

BIBLIOGRAFÍA

Aguilar, M., Gordillo, D., Paredes, J., C León, G. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 369-382. Obtenido de https://revistas.uh.cu/revflacso/article/view/3594

Alvear, G., C Pesantes, E. (2023). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos*. Cuenca: Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/25257/1/UPS-CT010631.pdf

Asamblea Nacional. (26 de Mayo de 2021). *finanzaspopulares.gob.ec*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asamblea Nacional del Ecuador. (2021, 27 de agosto). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Asamblea nacional . http://biblioteca.defensoria.gob.ec/handle/37000/3374

Asamblea Nacional del Ecuador. (2021, 27 de agosto). *Ley de Comercio Electronico, Firmas y Mensajes de Datos*. Asamblea Nacional del Ecuador. http://biblioteca.defensoria.gob.ec/handle/37000/3374

Blog Gobierno Corporativo. (21 de Septiembre de 2023). *Russell Bedford*. Obtenido de https://russellbedford.com.ec/ley-de-proteccion-de-datos-en-ecuador-guia-para-empresas/

Chicaiza Mullo, P. E. (2023). *La violación del derecho a la protección de datos de carácter personal*. Cuenca: Universidad Nacional de Chimborazo.

Clavijo, B. (2021). Investigación bibliográfica comparativa entre la efectividad del uso del. *UNIVERSIDAD CENTRAL DEL ECUADOR*, 1-80. https://www.dspace.uce.edu.ec/server/api/core/bitstreams/a5ede1d4-2b92-4b0c-a750-5997d93f6eb8/content

Córdova Hidalgo , H. L. (2020). *UMET UNIVERSIDAD METROPOLITANA*. Obtenido de file:///C:/Users/59399/Downloads/CORDOVA%20HIDALGO%20HUGO%20LEONIDAS-%20DERECHO%20(1).pdf

Corte Constitucional del Ecuador. (2021). *Corte constitucional del Ecuador*. https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=2064-14-EP/21

Del Pozo Basurto, H. (26 de Mayo de 2021). *finanzaspopulares.gob.ec*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Diario Oficial de la Unión Europea. (27 de Abril de 2016). *boe.es*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Dirección General de Mercado Interior . (6 de Julio de 2022). *Your Europe*. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

European Union. (2021). *European Commission*. Obtenido de European Commission: https://commission.europa.eu/law/law-topic/data-protection_en

Garrigues. (2018). *Garrigues*. https://www.garrigues.com/es_ES/noticia/regula-proteccion-datos-latinoamerica-influye-rgpd

Gomez, S. (2019). *Metodología de la investigación*. Estado de México: RED TERCER MILENIO S.C. https://dspace.itsjapon.edu.ec/jspui/bitstream/123456789/735/1/Metodologia_de_la_investigacion.pdf

González, P. (6 de Marzo de 2023). *PRIMICIAS*. https://www.primicias.ec/noticias/economia/empresas-ley-proteccion-datos-personales/

Google Spain SL. (28 de Noviembre de 2019). *FASKEN*. https://www.fasken.com/en/knowledge/2019/11/the-extra-territorial-scope-of-the-gdpr/

Grupo Bravco S.A. (19 de Mayo de 2023). *TEUNO*.

Guerra, M., C Navarrete, A. (2023). *Propuesta de un plan de cumplimiento del delegado de protección de datos en una empresa ecuatoriana de telecomunicaciones, 2022*.

Játiva Yánez, F. (31 de Marzo de 2023). *es.linkedin.com*. https://es.linkedin.com/pulse/la-madurez-del-ordenamiento-

jur%C3%ADdico-ecuatoriano-de-j%C3%A1tiva-y%C3%A1nez#:~:text=En%20cuanto%20a%20las%20diferencias,m%C3%A1s%20moderadas%2C%20estableciendoun%20r%C3%A9gimen%20m%C3%A1s

Javier, V. B. (2022). *Alcance de la protección de datos personales en el marco legal*. Guayaquil: Universidad Catolica de Guayaquil. http://repositorio.ucsg.edu.ec/bitstream/3317/18649/1/T-UCSG-PRE-JUR-DER-824.pdf

LEXIS . (28 de Agosto de 2023). *LEXIS Blog*. https://www.lexis.com.ec/blog/otros/lo-que-debes-saber-sobre-el-reglamento-general-de-proteccion-de-datos-rgpd

MICROLAB HARD S.L. (10 de Abril de 2023). *MICROLAB: protección de datos*. https://microlabhard.es/que-datos-protege-la-lopd-y-rgpd/#:~:text=La%20principal%20diferencia%20entre%20la,RGPD%20es%20un%20reglamento%20europeo.

Ministerio de Telecomunicaciones . (2019). *Gobierno electronico*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

Nisa Ávila, J. A. (8 de Octubre de 2020). *LEFEBVRE*. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

Ordoñez, L. (2021). *EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR*. Universidad de Cádiz. https://dialnet.unirioja.es/servlet/tesis?codigo=294113

Ordóñez, L., Correa, L., Correa , A. (15 de Julio de 2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. Loja, Ecuador: Estado C comunes, revista de políticas y problemas público.https://revistas.iaen.edu.ec/index.php/estado_comunes/article/view/270/470

Parlamento Europeo. (27 de Abril de 2016). *eur-lex.europa.eu*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02016R0679-20160504

Parlamento Europeo y Consejo de la Unión Europea . (27 de Abril de 2016). *boe.es*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Paz Canales , M., C Bordachar, M. (22 de Enero de 2021). *Derechos Digitales*. https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

Serrano, R. (9 de Noviembre de 2018). *Brasil ya se adaptó al RGPD ¿Ecuador será próximo?* https://revistagestion.ec/estrategia-analisis/brasil-ya-se-adapto-al-rgpd-ecuador-sera-proximo-opinion/

Enríquez, L. (15 de Junio de 2021). *La protección de datos en América latina: influencia del RGPD* https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/

Reyes Amán, J. G. (2016). *UDLA Repositorio*. file:///C:/Users/59399/Downloads/UDLA-EC-TAB-2016-29.pdf

UNIR REVISTA . (27 de Diciembre de 2021). *unir LA UNIVERSIDAD EN INTERNET* . https://www.unir.net/derecho/revista/reglamento-general-de-proteccion-de-datos/

Reglamento de la Ley Orgánica de protección de Datos. (13 de Noviembre de 2023). *Cosede*. https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf