Universidad Nacional de Loja

Facultad Jurídica Social y Administrativa

Carrera de Derecho

El tratamiento de Datos Personales y su Regulación Normativa en el Ecuador según las Nuevas Tecnologías de la Información y la Comunicación.

Trabajo de Titulación previo a la obtención del Título de Licenciada en Jurisprudencia y Título de Abogada

AUTORA:

Lady Carolina Pardo Guamán

DIRECTOR:

Dr. Jefferson Vicente Armijos Gallardo Mg.Sc.

Loja - Ecuador

2023

Loja, 27 de julio del 2023

DR. JEFERSON VICENTE ARMIJOS GALLARDO MG. SC

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Titulación denominado: **El Tratamiento de datos personales y su regulación normativa en el Ecuador según las nuevas tecnologías de la información y la comunicación**, previo a la obtención del título de **Licenciada en Jurisprudencia y Abogada**, de la autoría de la estudiante **Lady Carolina Pardo Guamán**, con cédula de identidad Nro. **1150097630**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

JEFERSON VICENTE ARMIJOS GALLARDO

Firmado digitalmente por JEFERSON VICENTE ARMIJOS GALLARDO
Fecha: 2023.07.21 16:34:58 -05'00'

Dr. Jeferson Vicente Armijos Gallardo Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

Autoría

Yo, **Lady Carolina Pardo Guamán**, declaro ser autora del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional - Biblioteca Virtual.

Firma: 

Cédula: 1150097630

Fecha: Loja, 21 de julio del 2023

Correo: lady.pardo@unl.edu.ec

Celular: 0994231062

Carta de autorización por parte de la autora, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo, del Trabajo de Titulación.

Yo, **Lady Carolina Pardo Guamán** declaro ser autora del Trabajo de Titulación denominado: **"El tratamiento de datos personales y su regulación normativa en el ecuador según las nuevas tecnologías de la información y la comunicación",** como requisito para optar por el título de **Licenciada en Jurisprudencia y Abogada**; autorizo al Sistema de Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 21 días del mes de julio de dos mil veintitrés.

Firma: 

Autor: Lady Carolina Pardo Guamán

Cedula No: 1150097630

Dirección: Loja- Catamayo

Correo Electrónico: ladypardo121298@gmail.com – lady.pardo@unl.edu.ec

Teléfono Celular: 0994231062

DATOS COMPLEMENTARIOS:

Director de trabajo de titulación: Dr. Jefferson Vicente Armijos Gallardo Mg.Sc.

Dedicatoria

La presente tesis está dedicada a Dios, ya que gracias a él he logrado concluir con mi carrera, a mis padres quienes me dieron la vida, educación porque ellos estuvieron a mi lado brindándome su apoyo y sus consejos para hacer de mí una mejor persona, a mis hermanos y sobrinos por sus palabras y compañía, a mi padrino y a toda su familia que se han convertido en mi segunda familia.

A mis compañeros y amigos quienes sin esperar nada a cambio compartieron su conocimiento, alegrías, tristezas y a todas aquellas personas que durante estos cinco años de carrera estuvieron a mi lado y lograron que esta meta se cumpla. Gracias a todos.

Lady Carolina Pardo Guamán

Agradecimiento

En primer lugar, gracias a Dios por el amor y la bondad que sin duda no tienen fin, me permites sonreír a todos mis logros que son resultado de tu ayuda, y cuando caigo y me pones a prueba aprendo de mis errores y cada día me vuelvo una mejor persona.

A la Universidad Nacional de Loja por haberme aceptado ser parte de parte de ella, a mis docentes quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, en especial al Doctor Jefferson Armijos Gallardo por la paciencia y los conocimientos otorgados.

Gracias a mis padres Carlos y Mercedes por ser los principales promotores de mis sueños, gracias ante todo por haberme dado la vida, por haberme enseñado cosas básicas del día a día como disfrutar de los pequeños detalles, por permitirme no tener miedo y, a la vez tenerlo cuando se necesita, por el apoyo brindado en cada etapa de mi vida, Gracias a ustedes el día de hoy es un sueño hecho realidad, me siento feliz por tenerlos junto a mí para compartir el final de una etapa importante en mi vida de estudiante. A ustedes expreso toda mi gratitud por el esfuerzo constante e incondicional para verme convertido en una profesional; como no agradecerles por el sacrificio económico y moral que he recibido de ustedes para cumplir mi meta, siempre dispuestos a sostenerme para no rendirme cuando veía mi camino difícil, mejores Padres no habría podido tener, me han enseñado a luchar por lo que quiero, respetando mis decisiones, aconsejándome y dejando que aprenda a volar con mis propias alas; a mis hermanos que como las ramas de un árbol crecemos en diferentes direcciones, pero nuestra raíz es una sola, en especial a mi hermana Viviana por ser mi confidente y mi cómplice, gracias a sus consejos, su compañía que llenaban de satisfacción mis días.

A mi padrino Jesús Pilco que siempre me ha brindado su confianza y su generosidad, por haber estado en buenos y malos momentos, ya que solo un ser de buen corazón puede dar lo mejor de sí mismo para ayudar a sus semejantes y dar sus valiosos consejos y buenos deseos en la vida de otra persona y eso es un gesto muy valioso para mí.

Finalmente, pido disculpas que amerita el caso a cada una de las personas quienes de alguna forma directa o indirectamente y aún sin saberlo han contribuido durante mi formación académica y sé que merecían un espacio en el presente apartado, muchas gracias a todos.

Lady Carolina Pardo Guamán

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

1. Titulo

“El tratamiento de datos personales y su regulación normativa en el Ecuador según las nuevas tecnologías de la información y la comunicación”

2. Resumen

Sírvase usted distinguido lector a profundizar en el presente trabajo investigativo intitulado: **"EL TRATAMIENTO DE DATOS PERSONALES Y SU REGULACIÓN NORMATIVA EN EL ECUADOR SEGÚN LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN"** El presente trabajo de investigación tiene como objetivo analizar los retos que genera la aplicación de la Ley Orgánica de Protección de Datos Personales en las empresas del sector privado ecuatoriano que realicen tratamiento de datos personales, pues la ley establece obligaciones para las compañías en su rol de responsables de datos, las cuales deben implementar una serie de medidas internas que contribuyan a una adecuada protección de los datos personales de los ciudadanos; para ello la ley establece un tiempo de dos años para que los responsables se adecuen a los preceptos establecidos dentro de las disposiciones, antes de que empiece a regir régimen sancionatorio, sin embargo el tiempo establecido por el legislador es insuficiente. Para ello se aplicó una metodología bajo el enfoque cualitativo, y como instrumento de recolección de datos se entrevistó a expertos en materia de protección de datos personales para conocer su opinión acerca de los retos que genera la implementación de la ley en los procesos internos de las empresas, con la finalidad de proponer reformas a las disposiciones transitorias de la Ley Orgánica de Protección de Datos Personales.

PALABRAS CLAVES: Datos Personales / Intimidad / Autodeterminación Informativa / Libertad De Información / Datos Automatizados.

2.1Abstract

Please, distinguished reader, to delve into this investigative work entitled: "THE TREATMENT OF PERSONAL DATA AND ITS REGULATION IN ECUADOR ACCORDING TO THE NEW INFORMATION TECHNOLOGIES AND THE COMMUNITY" The purpose of this research work is to analyze the challenges generated by the application of the Organic Law for the Protection of Personal Data in Ecuadorian private sector companies that treatment personal data, since the law establishes obligations for companies in their role as data controllers, which must implement a series of internal measures that contribute to an adequate protection of citizens' personal data; For this purpose, the law establishes a period of two years for those responsible to adapt to the precepts established within the provisions, before the sanctioning regime begins to apply; however, the time established by the legislator is insufficient. For this purpose, a qualitative approach methodology was applied, and as a data collection instrument, experts in the field of personal data protection were interviewed to know their opinion about the challenges generated by the implementation of the law in the internal processes of the companies, with the purpose of proposing reforms to the transitory provisions of the Organic Law for the Protection of Personal Data.

KEY WORDS: Personal Data / Privacy / Information Self-Determination / Freedom Of Information / Automated Data.

3. Introducción

El presente Trabajo de Titulación denominado: **"El tratamiento de datos personales y su regulación normativa en el Ecuador según las nuevas tecnologías de la información y la comunicación"** El progreso de la digitalización y las nuevas tecnologías han provocado que el mundo se encuentre cada vez más interconectado, y esto se evidencia en el aumento del intercambio fronterizo de datos personales que existe a nivel de empresas y países, resultado de la integración social y comercial que existe alrededor del mundo. En la actualidad los datos personales se han convertido en uno de los pilares sustanciales de las compañías en todo el mundo, pues debido a sus actividades de negocio recolectan, procesan y transfieren importantes cantidades de información de distinto tipo, entre ellas información personal. Con el tratamiento de este tipo de información personal, las empresas pueden evaluar tendencias y oportunidades de negocio, mejorar ventas, productividad, entre otros. Motivos por los cuales, es importante la regulación de un adecuado tratamiento, a través de derechos, principios, así como obligaciones, con la finalidad de tutelar el derecho a la protección de datos personales. En Ecuador el tratamiento de datos es regulado desde el 26 de mayo del año 2021 por la nueva "Ley Orgánica de Protección de Datos Personales", que si bien trae muchas garantías a los titulares de sus datos personales, es un hecho que plantea grandes retos a las empresas en su papel de responsable de datos, pues los encargados y/o responsables del tratamiento de datos personales deben implementar procedimientos y herramientas para dar cumplimiento a los requerimientos y obligaciones que dispone la ley. Por lo mencionado el presente trabajo de investigación tiene por objeto analizar los nuevos retos que enfrentan las empresas privadas ecuatorianas, que realicen TDP, a partir de la entrada en vigor de la Ley Orgánica de Protección de Datos Personales, con la finalidad de determinar las prácticas en materia jurídica de protección de datos que deben llevar a la práctica las compañías para dar

cumplimiento a la ley y evitar ser sancionados, así como generar confianza y una buena reputación para con otras compañías tanto a nivel nacional como internacional. Por lo expuesto este trabajo se ejecuta la fundamentación teórica de la investigación a través de los presupuestos sobre el objeto de estudio, en el marco teórico se expondrán definiciones de varios términos de carácter técnico muy utilizados en el sistema protección de datos, así como los marcos contextuales y marco legal, en donde se evidencia el objeto de la investigación desde la perspectiva de otros países con una normativa de datos más desarrollada. Posteriormente se establece el diseño de la investigación, en el que se determina el enfoque el cual es de tipo cualitativo, la aplicación de los tipos y métodos de investigación. En relación con las técnicas e instrumentos de recolección, utilizamos la entrevista como instrumento, en el cual se recogió la opinión de cuatro profesionales del derecho que trabajan en torno a datos personales, las cuales será de vital utilidad para el análisis planteado. Se encuentra redactada la propuesta para el problema planteado en el trabajo de investigación, la cual está enfocada en una reforma las disposiciones transitorias de la Ley Orgánica de Protección de Datos Personales, para sugerir una prórroga las medidas correctivas y régimen sancionatorio, así como establecer el tiempo para la expedición del reglamento a la ley y la institución de la Superintendencia de protección de datos. Finalmente, se culmina con las conclusiones al problema y las recomendaciones objeto del trabajo, así como con las referencias bibliográficas y anexos resultado de las fuentes utilizadas a lo largo del trabajo de investigación.

4. Marco Teórico

4.1 Datos Personales

Al hablar de datos personales podríamos referirnos en aspectos muy generales a un tipo de información, perteneciente o atribuible a una persona en específico. En este sentido los datos personales pueden ser entendidos, como información acerca de una persona que permite identificarla.

> Se considera dato personal a toda información numérica, alfabética, también imágenes (gráfica y fotográfica), acústica (sonidos y voces) o cualquier otro de tipo de información con las condiciones de que puedan ser recogidas, registradas, tratadas o transmitidas y que pertenezcan a una persona física identificada o identificable. Se anota que no solo se refiere a datos habituales o comunes, sino incluso a aquellos que la persona desconozca sobre sí misma, en virtud de la existencia de tratamientos como la minería de datos. (Santos García, 2012, pág. 15)

La LOPDP (2021) en su artículo número cuatro lo define como "Dato que identifica o hace identificable a una persona natural, directa o indirectamente" (Asamblea Nacional del Ecuador, 2021). Conceptos similares se encuentra en legislaciones comparadas sobre la materia, como el RGPD (2016) que considera dato personal "toda información relativa a una persona física identificada o identificable" (Parlamento Europeo, 2016).

En base a los conceptos anteriormente citados, es importante destacar que hay datos que por sus características, no hay una certeza cien por ciento confiable de que sean "personales", y en consecuencia deben ser analizados correctamente en el caso concreto, esto debido a que pueden existir dudas respecto a su vinculación con el individuo, dígase por ejemplo: correo electrónico, web e IP, log-in de acceso, SMS, etc.; por su parte, existen un grupo de datos que no admiten dudas

respecto de su naturaleza, y por ende, deberán gozar de un régimen de protección blindado, como por ejemplo: datos genéticos, datos de salud, datos obtenidos en sistema de videovigilancia, etc.

Teniendo claro lo que es un dato personal, se puede entonces entender que la persona natural o física es aquel ente propietario de sus datos, descartando así la protección de datos personales a las personas jurídicas.

Hay que tener en cuenta que los datos personales pueden ser: identificativos o identificables. Cuando hablamos de datos identificativos, nos referimos a:

> Aquellos que permiten una atribución directa como nombres, dirección, teléfono, número de cédula, pero también aquellos que se pueden sumar a los identificativos para someterlos a tratamiento (…) datos de características personales, datos de circunstancias sociales, datos académicos y profesionales, datos de detalles de empleo, datos de información comercial, datos económicos-financieros, datos de transacciones y datos especialmente protegidos. (Troncoso Reigada, 2010, pág. 12)

Se podría decir entonces que son aquellos datos personales ordinarios e incluyen cualquier tipo de información o identificadores que sirvan para identificar a una persona física. Este tipo de datos son relativamente fácil de conseguir, la identificación con el individuo puede ser indirecta, por ejemplo, ¿Podría identificar directamente a una persona usando solo el teléfono? Probablemente no, pues en ocasiones no existe la certeza de que determinado número de teléfono pertenezca efectivamente a una persona.

Por su parte, datos identificables son:

> Aquellos que para los que no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados y para determinar si una persona es identificable, hay que

considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. (Troncoso Reigada, 2010, pág. 13)

Un ejemplo de este tipo de tatos serían las huellas digitales, pues permite identificar directamente a un individuo, el riesgo de error es casi nulo.

Entonces, se puede concebir que los datos personales, son aquellos datos que sirven de información personal de identificación, ya sea directa o indirectamente, pero ¿a qué se refiere exactamente? "La información personal de identificación, también conocida como PII (del inglés *Personally Identifiable Information*), es todo conjunto de datos que pueden ser usados para identificar a un individuo en específico" (proofpoint, 2023, pág. 1). En sí, la identificación personal es en general un conjunto de datos, que aun por separado constituyen PII, se consideran datos delicados, y son la información que se usa en el robo de identidades, por lo que requieren de fuertes medidas de seguridad para la protección contra ataques

La Agencia Española de Protección de datos detalla que la información que puede ser asociada a una persona física concreta es:

> Nacimiento, matrimonio, domicilio, información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, información sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre las relaciones personales o sobre las creencias religiosas e ideologías, nombre y apellidos, números de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social. (Agencia Española de Protección de Datos, 2019, pág. 7)

A una persona se la puede asociar con algún tipo de información para poder realizar su identificación, como ya lo había manifestado en líneas anteriores, puede ser directa o indirectamente, lo que si es importante es que para su tratamiento debe hacerse tomando y aplicando las medidas de seguridad técnicas y organizativas necesarias para garantizar su protección y confidencialidad.

4.2 Derechos Digitales

Una definición de derechos digitales que sirve de referencia internacional es que:

> Los derechos digitales son los derechos de las personas en lo que respecta al acceso a ordenadores y la capacidad de usar, crear, y publicar medio digitales. Los derechos digitales también pueden referirse a los permisos permitidos para el uso justo de materiales digitales con derechos de autor. (Tech Target, 2017)

En los derechos digitales son una extensión de los derechos humanos como la libertad de expresión y el derecho a la privacidad, como se puede evidenciar en el anterior concepto los derechos digitales se relacionan con medios digitales, avances tecnológicos, datos, etc. Pero no solo podemos remitirnos a ese concepto, una concepción más generalizada y amplia es la que nos expresa Warkentin pues sostiene que los derechos digitales son “derechos exclusivos del ciberespacio (y específicamente el internet)” (Warketin, 2003, como se citó en Cova, 2010).

Para entender esta afirmación de Warketin es importante conocer lo que es el ciberespacio o derecho de internet que según Moisés Barrio se define como:

> El espacio global en el entorno de la sociedad de la información que consiste en el conjunto interdependiente de infraestructuras de las tecnologías de información y comunicación (TIC), y que incluye a internet, las redes de telecomunicaciones, los sistemas informáticos

y los procesadores y controladores integrados propios del internet. (Moisés Barrio, 2018, pág. 25)

Según lo manifestado por este autor, el ciberespacio ha revolucionado la comunicación debido a que se ha creado un entorno virtual que ofrece grandes beneficios y ventajas, pero también vulnerabilidades dando como resultado riesgos a la seguridad de los datos personales. Este escenario virtual, ha llevado al operador de justicia a definir los campos de actuación electrónica que tendría que aplicar en cada disciplina del derecho. Es una temática de suma importancia debido a que si seguimos el modelo generacional de los derechos humanos expuesto por Vasak estaríamos en presencia de una nueva generación de derechos específicamente la cuarta, la cual tal como lo manifestaba Bustamante "esta intrínsicamente relacionado con la capacitación de los ciudadanos para disfrutar de las posibilidades de realización personal que aportan las TIC" (Bustamante, 2007, pág. 63). Estos derechos de cuarta generación surgen gracias a las innovaciones tecnológicas como a la globalización. Es entonces un hecho tangible el surgimiento de nuevos escenarios donde es más necesario reconocer y garantizar los derechos digitales, que según la asociación para el progreso de las comunicaciones comprenden:

DERECHOS DE LOS USUARIOS DE INTERNET Y DE LAS TIC	
Intercambio de aprendizajes y creación de software libre y desarrollo tecnológico	
Acceso a internet para todos y todas	Privacidad, vigilancia y encriptación
Libertad de expresión y asociación	Gobernanza de internet
Acceso al conocimiento	Conciencia, protección y realización de los derechos

Tabla 1. Derechos digitales según la APC

Los derechos antes indicados son una muestra de cuán importante es reconocer y proteger a los usuarios, justamente la privacidad, vigilancia y la encriptación son clave dentro del tópico principal de la presente investigación.

4.3 Derecho a la Protección de Datos Personales

4.3.1 Reseña Histórica de la Protección de Datos Personales en el Derecho Comparado.

El derecho a la protección de datos personales tiene su génesis en el derecho a la intimidad, el cual parte del derecho norteamericano. Un punto de partida considerado a este concepto es al que los estadounidenses llamaron "*privacy*" en el estudio de un artículo denominado "*Warren-Brandeis article*"[1] en el año 1890. Pese a ello, algunos autores manifiestan que las primeras acepciones al derecho a la intimidad o privacidad, fueron obra del juez Thomas MacIntyre, el cual, en su destacada obra "*The elements of Torts*" define al derecho a la intimidad como "*the right to be let alone"*,[2] es decir, el derecho que tienen las personas a no ser perturbadas por interferencias externas no deseadas. (Eguiguren Praeli, s.f., pág. 94)

Entonces, según MacIntyre, la intimidad implica la ausencia de perturbaciones hacia la persona, para él, el intento de una agresión, un insulto, o inclusive, el simple hecho de infundir miedo, constituye como tal una transgresión a la intimidad.

No podemos pasar por alto, el hecho de que mucho antes de MacIntyre, en 1859 John Stuart Mill ya había estimado que "*over himself, over his own body and mind the individual is sovereign*" [sobre sí mismo, sobre su propio cuerpo y mente el individuo es soberano] (Stuart Mill, 1959). Básicamente, manifiesta la capacidad de autodeterminación e individualidad que es inherente de

[1] El artículo completo, escrito en inglés por Brandeis, Louis Dembitz puede ser consultado en el siguiente link: http://www.law.louisville.edu/library/collections/brandeis/node/225

[2] "*Personal immunity. — The right to one's person may be said to be a right to complete immunity; to be let alone"* [Inmunidad personal. — Puede decirse que el derecho a la propia persona es un derecho a la inmunidad completa; ser dejado solo.] (MacIntyre Cooley, 1895, pág. 9).

todo ser humano, la capacidad de dirigir, administrar y controlar nuestra vida sin la interferencia de otros.

Ahora bien, no podemos olvidarnos de que el derecho a la intimidad, ya fue sondeado por aportes filosóficos de autores anglosajones, que ya destacaban que todo individuo es libre en cuanto a su persona y capacidades, este individualismo es la médula del derecho a la intimidad, "En esta concepción liberal el derecho a la intimidad es básicamente una libertad negativa, un *estaus libertatis*, de no injerencia del estado o individuos en la subjetividad individual" (Eguiguren Praeli, s.f., pág. 94). Las concepciones de libertad positiva o negativa, tienen su origen intelectual en Benjamín Constant[3], posteriormente Isaiah Berlín desarrolló mas ideas en torno a esta concepción[4], básicamente, la libertad negativa es aquella que todos gozamos cuando nadie interfiere con nuestras acciones. En virtud de estos conceptos, la intimidad suponía el evitar la intromisión de agentes externos en la vida privada.

No podemos dejar de lado los aportes de Inglaterra, pues, Lord Mancroft en la década de los 60´ traslada la discusión sobre la privacidad e intimidad centrándolos en los conflictos con los medios masivos de comunicación, se podría decir, que fue él quien aportó por primera vez en Inglaterra conceptos sobre la "*privacy*" en la Cámara de los Lores, Hay que tener en cuenta los ingleses siempre han respetado férreamente la libertad de prensa, y el hecho de que Mancroft presentara con sus aliados un "proyecto de ley regulador del derecho a la privacidad se enfocaba en la simbiosis intimidad-privacidad y medios masivos de comunicación, los denominados "*mass media*", procurando proteger la privacidad de los datos de las personas frente a las publicaciones

[3] Constant fue quien introdujo novedosamente una distinción entre ambas formas de libertad, en su famoso discurso en el Ateneo de París en 1819, denominado: Sobre la Libertad de los Antiguos comparada con la de los Modernos. El discurso completo puede ser consultado traducido al idioma español en el siguiente link: https://educacion.uncuyo.edu.ar/upload/de-la-libertad-de-los-antiguos-comparada-con-la-de-los-modernos-benjamin-constant.pdf

[4] Berlín, en su famoso ensayo "Two concepts of Liberty" manifestó que: "Yo no soy libre en la medida que otros mi impiden lo que yo podría hacer si no me lo impidieran" (Berlin, 1967, págs. 141-152)

no consentidas" (Clímaco , 2012, pág. 28) provocó en respuesta un feroz ataque de la prensa en el que se llegaron a escribir artículos afirmando que el derecho o la libertad de prensa era el derecho por excelencia frente al que nadie podía competir. Por lo que, después de dos lectoras frente a la Cámara de Lores, y al sentir una oposición aplastante de la prensa y una falta de apoyo del Parlamento, Mancroft se dio por vencido manifestando: "(…) fui incapaz de establecer una distinción precisa entre lo que el público tiene derecho a conocer y lo que un hombre tiene derecho a conservar para sí mismo" (The Thimes, 1969, citado por Clímaco 2012).

Es evidente que Mancroft fracasó, pero, construyó ya los cimientos en el esquema de la protección de la privacidad en Inglaterra, que años mas tarde, daría como resultado la entrada en vigor de la Privacy Act. Pero no fue tan sencillo, surgieron después proyectos que, pese a que no prosperaron, abrieron debate para desarrollar el concepto de la privacidad en Inglaterra, tales como: Proyecto Lyon[5]; Proyecto Walden[6], este último influenció el pensamiento de crear un comité encargado de estudiar a fondo la *privacy*.

Se abordaron varios informes, en los cuales se trataba el tema de la privacidad y de una autoridad de control, luego de tantas discusiones y controversias, se obtuvo como resultado la denominada "*Data protection Act*" de 1984.

Posteriormente, tanto Francia como Alemania fueron incursionando en la materia. Como se puede observar, la sociedad ha ido evolucionando, y con ello todo lo relacionado a la libertad de información y expresión, y con ello se ha dado paso a derechos como el de la protección de datos personales.

[5] Según afirma Losano G. el objeto era "(…) proteger a la persona de toda interferencia irracional y seria que viole la separación entre lo público y la persona misma, su familia o su propiedad" (Losano G, 1989, pág. 18).
[6] "El objeto principal sería prevenir que se proporcionara información para un propósito específico y fuera usada para uno diferente desnaturalizándose, dándole así vida al principio que ahora se conoce como de finalidad" (Clímaco , 2012)

4.3.2 Intimidad Personal como antecedente al Derecho a la Protección de Datos Personales.

Para entender este apartado, es importante conocer el significado de intimidad, al cual La Real Academia española ha definido como: "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" (RAE, s.f.). Entonces, esta definición nos da la perspectiva de que es todo aquello relacionado con la vida privada, la cual no está exenta de sufrir perturbaciones. Esta concepción, tiene concordancia con lo que manifestaba el juez Cooley "to be alone". Entonces, desde un punto de vista jurídico, la intimidad es un derecho que tenemos todas las personas a poder desarrollarnos adecuadamente sin injerencias externas. Yendo mas allá, podemos citar a Adriano de Cupis, quien manifestaba que la intimidad es:

> Aquel modo de ser de la persona que consiste en la exclusión del conocimiento ajeno de cuanto hace referencia a la propia persona o también como la necesidad consistente en la exigencia de aislamiento moral, de no comunicación externa de cuanto concierne a la persona individual. (De Cupis, 1973, citado por Rebollo)

Hace referencia entonces al hecho de que tenemos el derecho de no comunicar a terceros aquellos detalles que pertenecen a nuestra vida personal, manifiesta que es una necesidad de asilamiento, es decir, de la no exigencia de un intercambio de pensamientos, de una incomunicación autoimpuesta con el individuo, nada tiene que ver con el aislamiento asociado a la falta de libertad, este tipo de aislamiento del que se habla en el concepto de intimidad es más bien una decisión que tiene como objetivo proteger nuestra vida privada.

Para 1983 el Tribunal Constitucional Alemán empieza a delimitar el contenido del derecho a la intimidad, a la cual define como: "la facultad del individuo, derivada de la idea de

autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida"[7] señalando además que:

> El que no pueda percibir con suficiente seguridad qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decir por autodeterminación. No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, que, cuando y con que motivo sabe algo sobre él. (…). Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos. (Ley del Censo, Derecho a la Personalidad y Dinidad Humana, 1983, pág. 27)

Manifiesta entonces que, el hecho de que un ciudadano se sienta inseguro dado que en todo momento se registren comportamientos divergentes, procurará no realizarlos, para no llamar la atención o para simplemente no meterse en problemas. Por lo tanto, el hecho de que la libre eclosión de la personalidad esté en juego, presupone que la protección de todos aquellos datos concernientes a la persona recaigan "por lo tanto, dentro del ámbito de derecho fundamental" (Ley del Censo, Derecho a la Personalidad y Dinidad Humana, 1983).

Como se puede observar, los alemanes desarrollan de muy buena manera el concepto de la intimidad relacionada con los datos personales, pues centra al derecho a la intimidad personal en

[7] "Este derecho a la autodeterminación informativa no está, sin embargo, garantizado sin límites" Sentencia del Tribunal Constitucional Alemán, 1983, Considerando C, II, 1b. La sentencia, traducida al idioma español, puede ser encontrada en el siguiente link: https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485

la faceta de decisión, control y vigilancia por parte de la persona titular, dándonos como resultado, el hecho de que los datos concernientes a la persona sean objeto de una tutela rigurosa al tratarse de un derecho fundamental.

Es importante aclarar entonces ¿qué es un derecho fundamental? Para el maestro Peces-Barba, cabe hablar de un derecho fundamental mediante la siguiente afirmación tripartita:

> 1. La exigencia moral; 2. La necesidad de que el Poder las asuma como suyas y las reconozca expresamente en un texto y 3. El elemento histórico, centrado en la variabilidad y evolución de la reflexión moral y de las circunstancias concretas que determinan las condiciones de vida existentes en un momento determinado. (Peces Barba, 1988, pág. 231)

Se puede afirmar entonces, que un derecho fundamental es aquel que incorpora la moral al derecho positivo a través de un fenómeno histórico. Es importante entonces conocer la evolución histórica de los derechos fundamentales, puesto que estos han surgido en base a las amenazas a las libertades o a la dignidad propia del ser humano. Ya nos decía el gran Robert Alexi, "El 'derecho' de una persona es aquello que le corresponde o que merece como persona y a lo que los demás están, por ello, obligados o sujetos a otorgarle o dejarle" (Alexy, 1993, pág. 174). Entonces un derecho fundamental es una facultad esencial de cada persona, los demás tienen la obligación de no perturbarle, por lo tanto, ante cualquier amenaza al mismo, debe existir una tutela jurídica, dada entonces por limitaciones establecidas en el ordenamiento jurídico.

En nuestro país, es la Constitución de 1998, quien en su artículo 23 reconoce el derecho a la intimidad, integrada con otros derechos de carácter personal, pues manifiesta que:

> (…) el Estado reconocerá y garantizará a las personas los siguientes: (…) 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La Ley protegerá el nombre, la imagen y la voy de la persona.

Es ya en la Constitución actual que se recoge el derecho a la intimidad personal como independiente, en su artículo 66: "Se reconoce y garantizará a las personas: 20. El derecho a la intimidad personal y familiar" (Asamblea Nacional del Ecuador, 2008). Considero que se dotó de autonomía a este derecho con el propósito de darle más énfasis debido a su importancia.

Entonces, la intimidad como derecho fundamental protege la esfera más privada del individuo. Acudiendo a la etimología de la palabra, intimidad proviene del latín "*intimus*" que significa "lo que está más adentro, lo más interior, el fondo", como lo definiría Quiroga Lavié:

> El respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas. (Quiroga Lavié, 1995, pág. 10)

Se evidencia entonces, que incluso, doctrinarios mas actuales, consideran a la intimidad en el marco de los autores anglosajones, el derecho a ser dejado solo, de tal manera de que cada persona pueda desarrollarse íntegramente sin perturbaciones externas.

Se evidenció en líneas anteriores que el derecho a la intimidad se encuentra bajo protección constitucional, sin embargo, tal como lo establecía el Tribunal Constitucional Alemán, no es absoluto, cosa similar pasa con los datos personales, se pueden ejercer bajo límites razonables que son impuestos en concordancia a los derechos de los demás, hablamos entonces de un interés público como justificación para sacrificar este derecho a la intimidad.

> Habrá entonces que ponderar siempre el interés público para justificar el sacrificio del derecho a la intimidad, integridad física versus las garantías constitucionales que perdería el individuo a cambio de la posible obtención de indicios probatorios que pueden llegar

incluso al esclarecimiento de situaciones jurídicas obscuras, sosteniendo que no se pueda llegar a la verdad material de otro modo. (Villalba Fiallos, 2017, pág. 8)

Entonces, siempre se deberá velar por el interés público, deberá existir una necesidad absoluta para tomar esta decisión, en este punto, el administrador de justicia deberá alcanzar una justificación constitucional objetiva y razonable.

La irrupción a gran escala de la informática y el manejo descontrolado de los datos personales, supuso un reto para los estudiosos del derecho, pues querían encontrar en que categoría del derecho encasillar la situación, en ese contexto, la intimidad se acomodó como la opción mas idónea para tutelar al individuo frente al uso de sus datos personales.

Cabe destacar, a consideración de esta autora, que es incorrecto manifestar que la intimidad y la protección de datos personales constituyen un único derecho, sin embargo, no podemos negar la evidente conexión que existe entre los mismos, como lo manifestaba Murillo de la Cueva:

> (…) si no coinciden los ámbitos que se quieren defender con el derecho a la intimidad y con la protección de datos personales; si aquél responde a una concepción preinformática, si ésta va configurándose como un sector especializado del ordenamiento jurídico cada vez más articulado y denso, tal vez convenga abandonar la referencia de la intimidad y encabezar la exposición de esta problemática con un epígrafe distinto. Como es evidente, no se trata únicamente de un cambio nominal, sino de una consideración sistemática, más acorde con la realidad.

Es así, que surge la necesidad de separar estos conceptos, caso contrario se produciría una contradicción terminológica importante, pues no solo se trata de datos íntimos en estricto sentido, sino también aquellos considerados no íntimos, desnaturalizando completamente lo que se c9oncibe como derecho a la intimidad. Es importante entonces tener en cuenta los cambios

producidos por la revolución informática, por lo que se debe velar que los datos personales sean dignos de tutela, puesto que revelan aspectos en general de la vida de una persona.

Se concluye entonces, que si bien es cierto, la protección de datos personales, surge como una categoría del derecho a la intimidad, es equívoco en la actualidad considerarlo de esa manera, puesto que se ha configurado como un derecho autónomo que posibilita a los titulares la tutela de la información suya que circula, constituyéndose en el eje central en torno al cual gira la relación existente entre las personas y la sociedad de la información y comunicación.

4.3.3 Derecho a la Protección de Datos Personales en Ecuador.

La Constitución de la República del Ecuador, reconoce la protección de datos personales como un derecho de libertad, así lo manifiesta:

Constitución, artículo 66, numeral 19:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Asamblea Nacional del Ecuador, 2008, pág. 30)

Como se puede observar, no solo prescribe el acceso a los datos, sino también, les otorga a los titulares la capacidad de acceder y accionar la norma para conocer su uso y finalidad, de tal manera de que puedan ser usados de manera legítima. Entonces, como lo decía Naranjo (2018), se puede afirmar que el objeto primordial de la protección de datos personales en nuestro país es proteger la autodeterminación informativa de la persona.

Con lo establecido en nuestra norma, no queda lugar a confusiones entre el derecho a la intimidad con la privacidad, dado que se protege todo tipo de datos personales, y se supera la

histórica barrera de la “intimidad” que únicamente protegía el dato íntimo, privado, reservado, personal, familiar o sensible, dando paso a la protección de una amplia gama de datos que a pesar de que se los puede considerar inocuos o irrelevantes, si no son tratados de forma adecuada pueden efectivamente afectar el libre desarrollo de la personalidad de un individuo, así como el ejercicio de otros derechos fundamentales.

4.4 Tratamiento de datos personales

La Ley Orgánica de Protección de Datos personales (2021) en su artículo 6 de definiciones estipula que el tratamiento es:

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales. (Asamblea Nacional del Ecuador, 2021)

En base a esta definición podemos extraer que el tratamiento es toda operación que se realice sobre los datos de carácter personal por medios automatizados, así como al tratamiento no automatizado. El tratamiento será automatizado cuando se encuentre en soportes informatizados a los que se accede mediante programas o sistemas informáticos, al contrario de los no automatizados o de carácter de manual en el que los datos se encuentran en documentación física; luego la ley menciona a los parcialmente automatizados en el que se combina el acceso informatizado con un almacenamiento de datos en soportes manuales.

En cuanto a las fases para el tratamiento de datos, Davara Rodríguez distingue tres:

> La toma de datos que se realiza sobre soportes de obtención de datos personales automatizados o no; la segunda fase es el tratamiento de datos en el sentido de que se realizan las operaciones enunciadas por la LOPDP sobre los datos; y finalmente la última fase es la utilización o comunicación. (Davara Rodriguez, 2006, pág. 69)

Estas fases son las que le dan sentido a la protección de datos personales como tal, no pueden existir una sin la otra, son complementarias, dado que no podemos tratar o utilizar datos si previamente no se los ha obtenido. Son fases que deben realizarse con el cuidado necesario para evitar la pérdida o mal manejo de los mismos.

El tratamiento de datos en actualidad representa una actividad cotidiana en todos los ámbitos y sectores de la sociedad, tanto en el privado como en el público. Es tan importante porque "todos requieren de la información personal para tomar y ejecutar decisiones de tipo económico, seguridad nacional, política, laboral, financiera, comercial, entre otros" (Razza, 2021, pág. 28). Para el sector privado como empresas y particulares los datos son de fundamental uso y permiten acceder y conocer al potencial cliente, colaborador o proveedor. Por ello la regulación no busca que no se traten los datos, por el contrario, lo que se quiere lograr es un tratamiento adecuado y conforme a la ley para evitar la vulneración de los derechos.

4.4.1 Fines de la Protección de Datos Personales

Cuando hablamos de protección de datos personales estamos hablando de los riesgos que pueden ocasionar la vulneración de este derecho, es por ello que es importante conocer el concepto de "riesgo" relacionado con la materia, Juan Francisco Rodríguez manifiesta que "En materia de protección de datos, el riesgo consistiría en la probabilidad de que suceda un daño para el

interesado como resultado de la realización de operaciones de tratamiento sobre sus datos personales" (Rodríguez, 2019, pág. 171).

De esta definición se puede dejar entrever los fines de la protección de datos personales, la cual, radicaría en la vulneración y en la violación de nuestros derechos y libertades fundamentales, produciéndonos así un daño, debido a la falta de un tratamiento adecuado. Es por ello que la Ley Orgánica de Protección de Datos Personales Establece que, su objeto y finalidad es:

> Garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (Asamblea Nacional del Ecuador, 2021)

La protección de datos personales se ha convertido en un tópico prioritario tanto para el sector público como para el sector privado. Estamos hablando de un derecho constitucional, que actualmente tiene su propia ley especial de protección, evidenciándose entonces la importancia que supone la protección de datos personales, el avance de las nuevas tecnologías no solo supone beneficios para los titulares y las empresas, también supone riesgos, debido a la vulnerabilidad que supone el manejo, a veces indiscriminado, de la información y los datos personales. Como destaca Rodríguez:

> Es fundamental tener en cuenta el riesgo que implica cualquier tratamiento de datos personales, así como cualquier otro riesgo que pueda derivarse de situaciones tales como violaciones de seguridad, que pueden acarrear daños y perjuicios físicos, materiales o inmateriales para las personas físicas, tales como pérdida de control sobre sus datos personales o limitaciones de sus derechos, discriminación, usurpación de identidad,

pérdidas financieras, reversión no autorizada de la seudonimización. (Rodríguez, 2019, pág. 172)

4.4.2 Principios Relativos al Tratamiento de Datos Personales

Si bien es cierto, el artículo 10 de la Ley Orgánica de Protección de Datos personales establece una serie de principios bajo los cuales se regirá, considero pertinente especificar los principios que son relativos al tratamiento de datos personales.

a) **Licitud, lealtad y transparencia:** los datos serán tratados de manera lícita, leal y transparente en relación con el interesado
b) **Limitación de la Finalidad:** los datos personales serán recogidos para fines determinados, explícitos y legítimos y no tratados ulteriormente de manera incompatible con dichos fines.
c) **Minimización de datos:** los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan.
d) **Exactitud:** serán exactos y, cuando sea necesario, actualizados; deben adoptarse todas las medidas razonables para garantizar que los datos personales que sean inexactos, habida cuenta de los fines para los que se tratan, se supriman o rectifiquen sin demora.
e) **Limitación del almacenamiento:** serán conservados en una forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines para los que se tratan los datos personales; los datos personales podrán conservarse durante períodos más largos en la medida en que los datos personales se traten únicamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

f) **Integridad y confidencialidad:** serán tratados de manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales, utilizando medidas técnicas u organizativas adecuadas. (General Data Protection Regulation, 2016, pág. 3)

Repasando uno a uno estos principios se puede decir que, respecto al primero, el procesamiento es legal si se basa en uno de los fundamentos legales enumerados en la normativa. El más destacado de estos fundamentos jurídicos es el consentimiento, pero también existen otros motivos, incluido el interés legítimo. La equidad debe interpretarse como una referencia al concepto general de justicia y equidad. El procesamiento no es justo si se lleva a cabo de una manera que pueda ser engañosa para el interesado o, incluso a pesar de su consentimiento, ser una amenaza para su privacidad. La transparencia por su parte, hace referencia a que el interesado debe recibir información sobre el tratamiento, independientemente del fundamento jurídico en el que se base el tratamiento e independientemente de si los datos se recopilaron directamente de él o se obtuvieron de otro modo.

El segundo principio, de limitación de la finalidad, se refiere a que el propósito del procesamiento se especificará antes de que comience el procesamiento y se respetará durante todo el ciclo de vida de los datos personales.

El tercer principio, minimización de datos, hace alusión a que los datos que no son necesarios para lograr el propósito previsto no pueden recopilarse, almacenarse o procesarse legalmente.

El cuarto principio, exactitud, está estrechamente relacionado con los derechos de acceso y rectificación de los interesados.

El quinto principio, limitación del almacenamiento, hace referencia a cuánto tiempo se puede almacenar un tipo particular de datos personales para un propósito particular. No más de lo necesario.

El sexto principio, integridad y confidencialidad, menciona la aplicabilidad de medidas de seguridad, las cuales son siempre necesarias siempre que se procesan datos personales; además, en ciertos casos específicos, puede aplicarse un estándar más alto. También debe tenerse en cuenta que garantizar la integridad de los datos de investigación también es un requisito de la ética y la deontología de la investigación.

4.4.3 Base de datos:

> Una base de datos es información que se configura para facilitar el acceso, la administración y la actualización. (…) Las bases de datos se utilizan para almacenar, mantener y acceder a cualquier tipo de datos. Recopilan información sobre personas, lugares o cosas. Esa información se reúne en un solo lugar para que pueda ser observada y analizada. Las bases de datos pueden considerarse como una colección organizada de información. (Lutkevich, s.f. , pág. 1)

Las bases de datos, como lo establece la definición anterior, funcionan como un catálogo de información asociada a un individuo, sus utilidades son variadas, las empresas las usan como un método para recopilar datos sobre procesos comerciales y de esta manera poder mejorarlos; los proveedores de atención médica utilizan bases de datos para almacenar de forma segura datos personales de salud para informar y mejorar la atención al paciente; y una de las bases de datos que a nivel mundial es utilizada por las personas, como lo es el almacenamiento en la nube. Como se puede evidenciar, las bases de datos, se utilizan para fines específicos, y siempre deben estar sujetas al consentimiento del individuo que brindó su información.

"Una base de datos es información que se configura para facilitar el acceso, la administración y la actualización" (Tech Target, 2017, pág. 1). Entonces, una base de datos no solamente es una bóveda en la que se almacenan datos, su propósito como tal es brindar un fácil acceso a la información que contiene, puede organizar los datos en tablas, filas, columnas e indexarlos para que sea más fácil encontrar información relevante, brindando paralelamente, un alto nivel de seguridad para evitar que los datos protegidos sean vulnerados.

4.4.4 Big Data

El término Big Data hace alusión al "(…) conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo" (Agencia Española de Protección de Datos, 2019, pág. 3). En otras palabras, es un conjunto de datos de gran tamaño y mayor complejidad, son voluminosos de tal manera que un software de procesamiento de datos convencional es incapaz de gestionarlos, dado que podría suponer decenas de terabytes a procesar. La variedad implica diversos tipos de datos disponibles no estructurados, como audio o video que requieren un procesamiento adicional para obtener su significado, así como también habilitar los metadatos.

"Cuando hablamos de Big Data no nos referimos únicamente a los datos, sino sobre todo a la capacidad de poderlos explotar para extraer información y conocimiento de valor para nuestro negocio" (Carisio, 2018, pág. 1). La Big Data les ofrece a las empresas la capacidad de recopilar lo que se denomina como "*insights*", de esta manera los algoritmos realizan el análisis de los datos, extrayendo información de valor para el negocio. Con lo anteriormente manifestado, se puede afirmar que Big Data no solo hace alusión a grandes volúmenes de datos a procesar, sino también,

a las técnicas de tratamiento específicas y eficientes que se utilicen para el manejo de la información.

4.4.5 Transferencia de datos

Para Razza (2021) “Es un proceso de exportación o importación de datos personales, contenidos en una base de datos ubicada en un Estado, que son enviados a otros Estados” (pág. 31). La transferencia de datos se refiere al intercambio seguro de archivos grandes entre sistemas u organizaciones, se utilizan a menudo para compartir datos empresariales seguros con un socio comercial. Debido a que los datos se mueven más allá del perímetro de la empresa, se debe tener cuidado para proteger los datos.

“La transferencia de datos se refiere a la recopilación, replicación y transmisión de grandes conjuntos de datos de una organización o unidad de negocio a otra” (informática, s.f., pág. 1). En un contexto interno, la transferencia de datos se utiliza a menudo como una alternativa a un sistema holístico de integración de aplicaciones empresariales. Sin embargo, la transferencia de datos se utiliza con mayor frecuencia para compartir datos de forma segura entre socios comerciales, proveedores o agencias gubernamentales con fines cooperativos.

4.5 Hábeas Data

4.5.1 Etimología del Habeas Data

La denominación Hábeas Data tiene sus antecedentes en la antiquísima garantía del hábeas corpus. La palabra latina “habeas” que proviene del latín *habere* que significa “téngase en posesión” junto con la palabra inglesa “data” que proviene de datum que significa dato, información. Por lo tanto, la frase Hábeas Data significa, literalmente, “traer los datos”, es decir, traer los datos personales del actor, a fin de que éste pueda conocerlos y resolver lo pertinente acerca de ellos.

Este es un mecanismo de acción que le da a la persona agraviada la posibilidad de acudir ante el sistema judicial para detener el abuso de datos personales. En general, permite al individuo acceder a información personal en bases de datos, la posibilidad de editar y actualizar datos, la posibilidad de asegurar que los datos sensibles mantengan su confidencialidad y la eliminación de datos personales sensibles que puedan violar el derecho a la privacidad

4.5.2 Finalidad del Habeas Data

Como muy bien lo manifiesta el doctor García Falconí, "el Hábeas Data resguarda la intangibilidad de la reserva de la vida privada del individuo y su entorno familiar" (García Falconí, como se citó en Chiriboga). Cuando pensamos en la recolección y resguardo de datos personales, generalmente consideramos a los sujetos de la recolección de datos como actores pasivos que, sin embargo, cuentan con marcos legales diseñados para la protección y tratamiento adecuado de sus datos. El habeas data otorga a estos sujetos la capacidad, a través del derecho de acceso, de rectificación y eliminación de los datos almacenados sobre ellos. La protección de datos es parte del habeas data y actúa tanto como un mecanismo de otorgamiento de derechos para las personas como una obligación por parte del Estado y sus instituciones. El cumplimiento está directamente relacionado con el derecho a la privacidad, así como al acceso a la información, ambos consagrados en diversos tratados internacionales.

Gracias a estas garantías constitucionales podemos indicar que la finalidad del Habeas Data es la protección de los datos personales ante el llamado poder informático. Se entiende la producción, almacenamiento y transferencia, de la información personal por instituciones públicos o privados, empresas y personas en general. En base a los avances tecnológicos que en la actualidad existen. La información que se maneja en el ámbito del llamado poder informático es impresionante, no solo por la rapidez con que ella puede ser transferida, sino el alcance, hasta

dónde pueden llegar nuestros datos, no solo hasta nuestro país sino en el mundo entero. Sin perjuicio que significa el registro de información falsa o errónea de la persona la manipulación de la información puede llevar consigo un grave riesgo para todos. (Habeas Data en el Ecuador, 2016)

En otras palabras, tiene como finalidad, proteger a la persona en su intimidad, además de garantizar el acceso y verificación de información, evitando que el ciudadano sea violentado en sus datos por el Estado o particulares.

4.6.3 Habeas Data y la Protección de datos personales.

Con el mundo cada vez más experto en tecnología, el peligro del mal uso de los datos se ha convertido en una seria preocupación para la seguridad y la privacidad de las personas. El Habeas Data ha cobrado importancia en la creación de medidas de seguridad efectivas y el involucramiento del gobierno en la regulación de los mecanismos de protección de datos, los cuales son primordiales si se desea acceder, utilizar o almacenar información para su resguardo.

El Habeas Data, como se aclaró anteriormente, se refiere al derecho legal de un ciudadano sobre su propia información. La protección de datos denota cómo se debe obtener, procesar y salvaguardar la información.

Cuando se trata de privacidad de la información, “la realidad es más compleja, las leyes de privacidad y derecho a la información actúan como derechos complementarios que promueven los derechos de las personas a protegerse y promover la responsabilidad del gobierno” (Banizar, 2011). Como tal, la privacidad está siendo cuestionada constantemente por las tecnologías cambiantes y, en respuesta a esas modificaciones, “más de 60 países han adoptado leyes integrales que otorgan a las personas cierto control sobre la recopilación y el uso de datos por parte de organismos públicos y privados” (Banizar, 2011). Sin embargo, el acceso a los datos es cada vez más fácil gracias a estas nuevas tecnologías, donde una persona puede buscar sus propios registros

sin mayores problemas. Por lo tanto, los organismos e instituciones gubernamentales están diseñando nuevos estándares de protección de datos que son más detallados que nunca, un ejemplo de ello es la Ley Orgánica de Protección de Datos Personales.

4.6 Realidad actual respecto de la Protección de Datos Personales en el Ecuador

Partiendo del hecho de que las normas jurídicas surgen en respuesta a la realidad social, es importante preguntarnos ¿por qué en el Ecuador anteriormente no fue una necesidad social la creación de una norma que proteja los datos personales? No existe una respuesta concreta, es factible afirmar que sería una responsabilidad compartida entre el Estado, las empresas y los ciudadanos, pues debió haberse exigido una ley que delimite el ejercicio de este derecho.

> La protección de datos personales en nuestro país se dio a través de tres etapas:
>
> Primero, la protección constitucional por medio del habeas data; segundo, la regulación de la información personal y de la intimidad con una perspectiva garantista mediante leyes sectoriales; tercero, el reconocimiento de un derecho fundamental a la protección de datos personales en la Constitución de 2008. (Ordoñez Pineda, Correa Quezada, & Correa, 2022, pág. 1)

Es así, que en el año 2019 el entonces presidente de la República Lenin Moreno, envió a la Asamblea Nacional El Proyecto de Ley Orgánica de Protección de Datos Personales, que fue finalmente aprobado en mayo de 2021, esta ley norma el tratamiento de datos personales realizado por empresas a fin de garantizar el derecho constitucional de protección de datos, dando paso a una cuarta etapa en nuestro país.

La mencionada Ley está dividida en XII capítulos y más de setenta artículos. Pero, es pertinente centrarnos en los capítulos que abordan el tópico principal de la presente Tesis, los

cuales son el capítulo VI el cual trata las medidas de seguridad aplicativas y el capítulo VII en el cual se establecen los roles y responsabilidades en materia de protección de Datos Personales.

4.6.1 Elementos del sistema de protección de datos personales.

La Ley Orgánica de Protección de datos personales especifica claramente los elementos que componen e intervienen en el sistema de protección de datos ecuatoriano.

4.6.1.1 Titular.

El titular de los datos personales básicamente es la persona física a quien pertenecen y se refieren los datos personales, la LOPDP en su artículo 4 lo define como "Persona natural cuyos datos son objeto de tratamiento" (Asamblea Nacional del Ecuador, 2021, pág. 7). Como ya se había manifestado anteriormente, se excluyen a las personas jurídicas. El titular es el dueño de los datos personales, sin perjuicio de que estos se encuentren en posesión de un tercero para su tratamiento.

4.6.1.2 Responsable de tratamiento de datos personales.

Es aquella "persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales" (Asamblea Nacional del Ecuador, 2021, pág. 7). Es entonces el encargado de decidir sobre el tratamiento de los datos personales, estableciendo las finalidades del tratamiento o el uso que les dará, el tipo de datos que se requieren, la forma en que se obtienen, almacenan y suprimen, cuales serían los casos en los que se pueden divulgar etc.

4.6.1.3 Encargado del tratamiento de datos personales.

Según la LOPDP es aquella "Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales" (Asamblea Nacional del

Ecuador, 2021, pág. 7). A diferencia del anterior, el encargado no decide que hacer o como usar los datos personales, únicamente se encarga de emplearlos según las instrucciones que de el responsable.

4.6.1.4 Destinatario.

"Persona natural o jurídica que ha sido comunicada con datos personales" (Asamblea Nacional del Ecuador, 2021, pág. 7). Cabe destacar, que según la Unión Europea manifiesta que no serán considerados destinatarios cuando se transmitan datos a las autoridades públicas.

4.6.1.5 Delegado de protección de datos.

El delegado según la Ley Orgánica de Protección de Datos Personales es aquella:

> Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos. (Asamblea Nacional del Ecuador, 2021, pág. 7).

Se evidencia entonces, la gran importancia del rol de esta persona, debido a que el actuar conforme a la normativa de la persona natural o jurídica, pública o privada, responsable o encargada del tratamiento, depende de su asesoría y gestión.

4.6.1.6 Autoridad de Protección de Datos Personales.

Será aquella "Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales" (Asamblea Nacional del Ecuador, 2021, pág. 6). A la fecha, la plataforma el Consejo de Participación Ciudadana y Control Social señala 'en proceso' la presentación de una terna de

candidatas que puedan ser evaluadas por una comisión técnica, por lo tanto, aun no contamos con la Autoridad de Protección de Datos.

Según señala la información emitida por el Consejo, el procedimiento se encuentra desde mediados del año pasado en el despacho presidencial de Guillermo Lasso, aguardando la nominación de una terna por su parte. (CPCCS, s.f.)

Es así, que los responsables de datos personales deberán enfrentar un gran reto, esto debido a que aún no existe una autoridad a la cual puedan acudir para resolver dudas en torno a la Ley.

4.7 Medidas de Seguridad

Se entiende por medidas de seguridad a la materialización de esfuerzos para la debida protección de datos personales, que contribuyen con el efectivo ejercicio del derecho constitucional a la protección de datos personales.

Entonces, para efectivizar la protección de datos personales, las empresas están obligadas a emplear controles y mecanismos de seguridad para mitigar amenazas o riesgos. La legislación ecuatoriana establece la obligación de tomar medidas, las cuales son de cinco tipos: administrativas, técnicas, físicas, organizativas y jurídicas.

La seguridad de la información se articula en tres dimensiones:

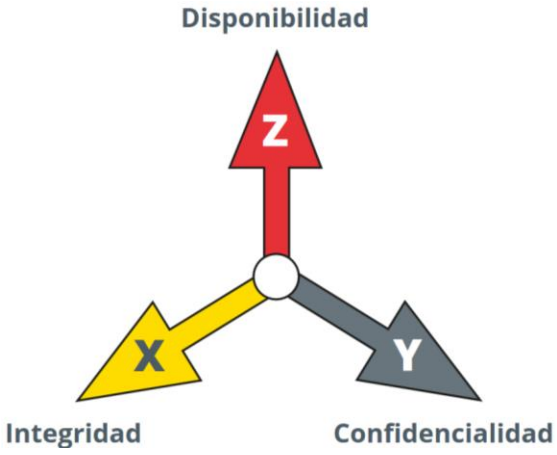


Figura 1. Dimensiones de la seguridad de la información.
Fuente: Instituto Nacional de Ciberseguridad de España

La disponibilidad de la información se refiere a “que la información esté accesible cuando la necesitemos” (Instituto Nacional de Ciberseguridad, s.f., pág. 6). Es por ello que se deberán disponer de métodos razonables y eficientes que permitan a las personas cuyos datos personales han sido recopilados, puedan solicitar su acceso.

La integridad, por su parte, se refiere a “que la información sea correcta y esté libre de modificaciones y errores” (Instituto Nacional de Ciberseguridad, s.f., pág. 6). La información puede ser modificada intencionalmente o simplemente puede ser incorrecta, es por ello que se deberá revisar minuciosamente que los datos se mantengan exactos, completos y actualizados.

Y, por último, la confidencialidad “implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como *need-to-know*” (Instituto Nacional de Ciberseguridad, s.f., pág. 6). Básicamente, se hace alusión a que los datos no deben divulgarse o ponerse a disposición de terceros, mucho menos utilizarse para otras finalidades alejadas a las que se recopilaron, a excepción del consentimiento del titular o la ley.

Una vez hemos conocido las dimensiones de la seguridad de la información, es importante conocer las diversas medidas de seguridad que se aplicarán para protegerlas en pro del correcto ejercicio del derecho a la protección de datos, destacando siempre que estarán ligadas a las circunstancias propias de las empresas, dependiendo de su giro de negocio y desarrollo de actividades.

4.7.1 Medidas de seguridad técnicas

Las medidas de seguridad técnicas son “el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software, para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento” (IDAIP, s.f., pág. 13). Estas medidas, se

pueden aplicar a los sistemas de datos personales contenidos en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información.

Las medidas de seguridad técnica podrán prever las siguientes acciones:

- **Gestión de comunicaciones y operaciones.** Es establecer controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna, como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento. (IDAIP, s.f., pág. 14)

En el nivel más básico, los cortafuegos, los análisis de malware, la protección antivirus, los parches y la actualización del software cuando sea necesario son las medidas técnicas de seguridad más comunes que se aplican para proteger los datos personales que procesa contra ataques cibernéticos.

- **Control de acceso.** Se deberá establecer medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información. (IDAIP, s.f., pág. 14)

Los responsables de los datos están obligado a evitar la intrusión de personas no autorizadas en los sistemas y aplicaciones utilizados para el procesamiento de datos personales. Para garantizar esto, se procura otorgar acceso a los sistemas de procesamiento de datos del titular únicamente a los administradores autorizados explícitamente.

- **Adquisición, desarrollo, uso y mantenimiento de sistemas de información.** Relativo a la Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera el procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros. (IDAIP, s.f., pág. 14)

Básicamente se refiere al servicio técnico que se le deberá otorgar constantemente a los equipos informáticos en los cuales se almacena la información de los titulares. El control de información es muy estricto, por lo cual debe ser revisado continuamente, ello con el afán de proteger la confidencialidad, autenticidad o integridad de la información.

4.7.2 Medidas de Seguridad Físicas

"Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento" (IDAIP, s.f., pág. 15). Básicamente, se enfocan en lo relacionado a los controles de mantenimiento y soporte técnico de todos aquellos equipos que contienen datos personales; a prevenir un acceso no autorizado a perímetros e instalaciones que se consideren áreas críticas de recursos e información; a prevenir el daño e interferencia a las instalaciones físicas; y, también, proteger los recursos móviles, que puedan salir de las instalaciones de la empresa.

4.7.3 Medidas de Seguridad Administrativas

Estas medidas se refieren a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales. (IDAIP, s.f., pág. 16)

Las medidas de seguridad anteriormente mencionadas aludían a lo que se debe realizar a nivel tecnológico o físico para asegurar la protección de datos personales, en cambio, las medidas administrativas se enfocan en la empresa como tal, tanto de sus directivos como de sus empleados.

Se pueden considerar medidas de seguridad administrativas las siguientes:

- **Política de seguridad.** Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado. (IDAIP, s.f., pág. 16)

Las políticas de seguridad de una empresa, según la definición anterior, son requisitos escritos que los empleados deben seguir. Por lo general, cada política de empresa aborda un único punto clave de preocupación. Eso mantiene la información dentro de una política cohesiva, asegurando que los detalles necesarios estén bien cubiertos y limitando los malentendidos relacionados con el tema.

- **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones a la normatividad vigente, o la política de seguridad interna u obligaciones contractuales. Abarca, entre otros, el cumplimiento y la identificación de requerimientos tales como la legislación aplicable al sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal. (IDAIP, s.f., pág. 16)

Es importante aclarar que, tener políticas y procedimientos establecidos no es suficiente. Es necesario asegurarse de que sean efectivos. Por ello, es importante establecer controles y auditorías para evaluar la eficacia, la debida aplicación de la normativa para evitar incurrir en infracciones, y en general corregir lo que no funciona y mejorar lo que se podría haber hecho mejor.

- **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros. (IDAIP, s.f., pág. 17)

El principal objetivo es proteger los datos personales contra la destrucción o pérdida accidental. A tal efecto, la arquitectura de los sistemas de procesamiento de datos de la empresa, incluida la infraestructura de red, la fuente de alimentación y la conexión a Internet, deben diseñarse de con minucioso cuidado, del mismo modo, el tratamiento de los datos deben realizarlo las personas expresamente designadas y calificadas para tal efecto, evitando así afectar al titular o a un tercero.

- **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable. (IDAIP, s.f., pág. 17)

El control y clasificación de activos, es una tarea que debe realizarla un profesional en el área, el cual debe asegurarse de que la organización para la que trabajan identifique y clasifique correctamente toda la información y los activos de la organización. Para realizar la identificación de información y activos, los profesionales de seguridad de datos deben trabajar con los representantes de cada departamento o área funcional. Después de identificar la información y los activos, se deberá realizar la clasificación de datos y activos y documentar la sensibilidad y la criticidad de los datos.

- **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral. (IDAIP, s.f., pág. 17)

Abarca el desarrollo de una cultura de concienciación sobre seguridad y protección de datos garantiza para que los empleados conozcan los requisitos legales y lo que se espera de ellos. La seguridad y la protección de datos no es una tarea de una sola persona, cada trabajador tiene un rol, un papel que desempeñar. La formación periódica y continua, así como las actividades de sensibilización, pueden ser una medida eficaz.

- **Administración de incidentes.** Implementación de controles enfocado a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información. (IDAIP, s.f., pág. 17)

En otras palabras, se refiere a una evaluación de riesgos, considerado fundamental dentro de cualquier empresa que tome responsabilidad en el manejo de datos personales, esto debido a que las evaluaciones de riesgos permiten desarrollar soluciones de mitigación por lo cual pueden constituir una medida preventiva eficaz.

- **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye la planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado. (IDAIP, s.f., págs. 16-17)

En esencia, se refiere al nivel de preparación de una empresa para mantener funciones críticas después de una emergencia o interrupción, como por ejemplo: brechas de seguridad; desastres naturales; cortes de energía; fallas de equipos; salida repentina del personal; etc.

4.7.4 Medidas de seguridad jurídicas

Las medidas jurídicas, no son otra cosa que las acciones que tomarán las empresas para cumplir con lo establecido en la Ley Orgánica de Protección de Datos Personales, como por ejemplo, la designación del delegado, responsable o encargado del tratamiento de datos personales, dado que los roles de estas personas son muy importantes, pues de la calidad de su gestión depende que se cumpla con los estándares que establece la normativa.

> (...). Las obligaciones legales corporativas para implementar medidas de seguridad se establecen en un mosaico cada vez mayor de leyes, reglamentos y acciones de ejecución estatales, federales e internacionales generalmente aplicables, así como deberes de derecho consuetudinario y otras obligaciones expresas e implícitas para proporciones 'razonables'" o seguridad "adecuada" para los datos corporativos. (…). (Smedinghoff, 2019, pág. 4)

Tenemos que tener en cuenta, que la seguridad de datos personales abarca un amplia gama de ámbitos que no se pueden abarcar en una sola ley, sino que se contempla mas normativa, con la finalidad de salvaguardar la integridad de los datos de los titulares, es por ello que las medidas de seguridad jurídicas son parte esencial en la protección de información, no solo la LOPDP funciona como instrumento legal, también se lo podría considerar una medida de seguridad preventiva, sin perjuicio de los reglamentos internos de cada empresa, y lo establecido a nivel constitucional e instrumentos internacionales.

4.8 Consecuencias por vulnerar el derecho a la protección de datos personales

De darse el caso en que se incurra en violación a la seguridad de los datos personales o no se cumpla con las disposiciones legales establecidas, se sancionará al responsable y al encargado del tratamiento que hayan incumplido la norma, o bien, que bajo su responsabilidad se hayan vulnerado los derechos de los titulares.

La Ley Orgánica de Protección de Datos Personales prevé acciones administrativas que le otorgan al titular la capacidad de ejercer sus derechos y poder accionar mediante la autoridad competente las sanciones correspondientes, sin dejar de lado de poder acceder a otras vías judiciales.

4.8.1 Exigencias de la LOPDP para resguardar la seguridad de datos personales

Se destaca que la LOPDP implementa a la seguridad de los datos personales como un principio (artículo 10, literal j) el cual se observará en todo momento al tratar los datos personales. Del mismo modo, desarrolla dentro de su capítulo VI una serie de obligaciones que las empresas deberán cumplir.

"Garantizar la "confidencialidad, integridad, disponibilidad" y "resiliencia" de los datos personales" (Parlamento Europeo, 2016). Los datos personales ostentan de una gran importancia a nivel de las empresas, por lo cual su tratamiento debe realizarse en base a parámetros como la confidencialidad, que básicamente se refiere a cómo se manejará, administrará y difundirá la información privada de identificación.; la integridad se refiere a que se debe garantizar que los datos sean válidos y precisos en todo momento, y cualquier tipo de modificación debe ser siempre autorizada por el titular; la disponibilidad, hace referencia a el acceso a los datos, a que debe estar a disposición a quienes quieran hacer uso de ellos, siempre y cuando sea autorizado; y, por último la resiliencia de los datos, hace referencia a la capacidad de datos para estar disponibles tanto a aplicaciones o personas, la capacidad que tienen estos de adaptarse a los requerimientos e incluso a fallos del sistema, para evitar perjudicar la información de los titulares.

Adoptar, para poder garantizar lo señalado en el numeral 1, "todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole" (artículo 10 literal j LOPDP). En general, como

responsable del tratamiento, las empresas tienen la obligación de garantizar la seguridad de los datos personales, de acuerdo con el principio de integridad y confidencialidad. Tener las medidas apropiadas ayudará a prevenir violaciones de datos y cumplir con el principio de protección de datos. Tales medidas ya han sido tratadas anteriormente en el presente trabajo de titulación, tales como medidas de seguridad técnicas, medidas de seguridad organizativas, medidas de seguridad jurídicas, y medidas de seguridad físicas.

Las medidas referidas deben determinarse caso a caso y a la medida de su organización a fin de gestionar adecuadamente el riesgo. Para elegir dichas medidas debe:

> Tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos. (artículo 37 LOPDP).

La cantidad de datos que son generados cada segundo, cada minuto, cada hora, no pueden tener similar tratamiento, debido a que no es lo mismo, una base de datos que administra un volumen menor, a un Big Data, que las cantidades son exponencialmente mayores, es por ello que las empresas deben procurar el desarrollo de un software adecuado a cada situación, tomando en cuenta los costos de la misma y la importancia de la información, evitando así menoscabar datos de los titulares.

Requiere, además, implementar procesos de monitoreo (“de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad”) y mejora continua de las medidas adoptadas (artículo 37 LOPDP). Los datos deben ser monitoreados, es decir, se deberán usar herramientas y tecnologías para proporcionar una visibilidad continua de quién accede a qué datos y cómo los está usando; por su parte, la verificación, evaluación y valoración

continua y permanente prevé que se deberá usar respaldos para verificar los datos personales a través de una copia y determinar efectivamente que sean auténticos, del mismo modo, se deberá procurar que las medidas de seguridad sean capaces de reducir riesgos en el tratamiento de datos personales, en general, de cumplir con las expectativas para lo cual fueron establecidas.

La metodología de gestión del riesgo que requiere emplear para determinar sus medidas (numeral 2) y como parte de los procesos de monitoreo y mejora continua (numeral 4), debe ser adecuada y considerar: "el impacto en los derechos y libertades de los titulares de los datos" (artículo 41 LOPDP). Las medidas de seguridad tienen un impacto positivo en el tratamiento de datos personales, esto debido a que los protegen de posibles ataques o en casos mas extremos de ser susceptibles de delitos informáticos, pero hay que tener en cuenta que estas medidas de seguridad en ningún momento deberán colisionar con los derechos de los titulares de acceder, actualizar y modificar datos cuando fuere necesario.

Es necesario que sea capaz de "evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados" (artículo 37 LOPDP). La privacidad de los datos es vista como un derecho fundamental, por lo que toda acción lesiva debe evitarse en cualquier momento y costo. Las medidas de seguridad juegan un papel crucial en la protección de datos, ya que son una herramienta clave para ajustar la implementación de todas las leyes y requisitos de privacidad necesarios, así como para priorizar las acciones de dichas leyes y procesos.

La vulneración de la seguridad de datos personales debe notificarse a la Autoridad de Protección y al titular de los datos personales, en los casos y forma previstos en los artículos 43 y 46 de la LOPDP.

4.8.2 Régimen sancionatorio en materia de datos personales

Como se puede observar en el apartado anterior, las obligaciones recogidas no son completamente específicas, más bien, son amplias y está el hecho de que no existe específicament3 un manual de instrucciones de las medidas que se debe implementar.

Esta forma de establecer obligaciones es a mi consideración, contraproducente, esto debido a que nuestra normativa está adoptando un paradigma europeo, es decir "una aproximación centrada en el riesgo, es decir, no establece un checklist de medidas obligatorias, sino que deja que cada organización escoja las 'adecuadas y necesarias'" (Bodero & Asociados, 2022). En otras palabras, deja a albedrío de la compañía la implementación de sus medidas en base a su realidad y a un proceso de gestión de riesgo.

Las sanciones administrativas que establece la LOPDP para las empresas en caso de infracción o incumplimiento de sus disposiciones, deberán ser aplicadas por la Autoridad de Datos Personales tal como lo establecen los artículos de 65 al 72.

Existen dos tipos de infracciones en las cuales actuará el régimen sancionatorio. Las infracciones leves y graves. Las multas que se establecieron para las mismas son:

- **Infracciones leves:** multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.
- **Infracciones graves:** multa de entre el 0.7% y el 1% del volumen de negocio correspondiente al ejercicio económico inmediatamente anterior.

Para mejor comprensión, la LOPDP define al volumen de negocio como: "cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del

IVA y de otros impuestos directamente relacionados con la operación económica" (Asamblea Nacional del Ecuador, 2021, pág. 35).

El régimen sancionatorio de la LOPDP no está solamente conformado por multas, sino también por la imposición de medidas correctivas, esto como una manera de evitar que la conducta se siga perpetrando y prevenir que se produzca nuevamente.

4.9 Medidas correctivas

Se podría afirmar que las medidas correctivas son "un acto procedimental que tiene por finalidad revertir los efectos que la conducta infractora hubiera ocasionado o evitar que ésta se produzca nuevamente en el futuro" (Villanueva Haro, 2007, pág. 12). Entonces, hablamos de que las medidas correctivas buscan restablecer la legalidad alterada por el acto ilícito. La LOPDP establece que la Autoridad de Protección de Datos Personales en el caso de infracciones leves "(…) activará directamente el procedimiento administrativo sancionatorio, haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida"; por su parte, si se tratase de una infracción grave "(…) aplicará en primera instancia medidas correctivas" si estas fueren cumplidas de forma tardía, parcial o defectuosa, se procederá como en las otras infracciones; y, si se tratase de una infracción muy grave "(…) activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida" (Asamblea Nacional del Ecuador, 2021).

Por lo general, se concebía a las medidas correctivas como poseedoras de una individualidad que otro tipo de medidas no presumen, pues no dependían de un procedimiento en curso, o de futuras medidas, más bien estaban destinadas a concluir con el estado de cosas y efectos ilegales, sin la necesidad de aperturar previamente un procedimiento sancionador, pero, como se

puede apreciar, la LOPDP se desliga un poco de este clásico concepto, incluyendo a las medidas correctivas como parte de un procedimiento administrativo sancionador.

El artículo 65 de la LOPDP manifiesta que las medidas correctivas podrán consistir entre otras en:

- El cese del tratamiento, bajo determinadas condiciones o plazos;
- La eliminación de los datos; y
- La imposición de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales. (Asamblea Nacional del Ecuador, 2021)

Se considera que el incumplimiento de estas medidas es causal factible para el posterior establecimiento de multas, es decir, la transgresión de las mismas solamente agravará la situación, de quien ya, de primera mano, incumplió la norma.

4.10 Vías Judiciales Alternativas

Como ya se había manifestado con anterioridad, la vulneración al derecho de la protección de datos personales, además de el régimen sancionatorio a quienes tratan los datos personales, proporciona la oportunidad al titular de acceder a otras vías para hacer valer sus derechos.

4.10.1 Vía Civil.

El titular puede demandar al responsable o encargado del tratamiento por daños y perjuicios, esto a consecuencia de que sus intereses fueron afectados, así como buscar la debida reparación por los perjuicios que se le ocasionaron. Tal como lo establece el Reglamento General de Protección de Datos del Parlamento Europeo en su artículo 146 “El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento” de tal manera que

“Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos” (Parlamento Europeo, 2016, pág. 27).

Si una empresa sufre una brecha de seguridad y se exponen datos personales, es indispensable determinar que datos fueron expuestos para cuantificar el daño, es un asunto que puede ser ventilado por la vía civil mediante la cual el titular deberá demostrar el daño y perjuicio que ha causado la filtración de sus datos personales.

4.10.2. Vía Penal

El control punitivo del Estado se extiende a la protección de los datos personales, pues dentro del Código Orgánico Integral Penal se tipifican ciertos delitos relacionados a la privacidad de los datos personales, se pueden mencionar:

- Violación a la Intimidad (COIP, artículo 178)
- Intercambio, comercialización o compra de información de equipos terminales móviles (COIP, artículo 192)
- Revelación ilegal de base de datos (COIP, artículo 229)
- Falsificación informática (COIP, artículo 234, numeral 1)

El avance tecnológico ha sido tan importante en materia de datos personales y su tratamiento, pues ha permitido que exista una facilidad para tratarlos y protegerlos, pese a ello, así como avanza la tecnología, surgen nuevas formas de afectación a la información. Los delitos informáticos dependerán de “la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas” (Camacho, como se citó en Acurio).

Es por ello que, para minimizar la comisión de estos delitos, las medidas de seguridad que adopte cada empresa deberán ser las adecuadas y cumplir con estrictos parámetros de control en el manejo de información.

4.10.3 Vía Constitucional

La protección de datos personales en nuestro país, antes del 2021 no contaba con una norma específica, pero el derecho a la protección de datos personales ya se encontraba dentro de la Constitución, así como también la garantía jurisdiccional del Hábeas Data, que como ya se había tratado con anterioridad en el presente trabajo investigativo, permite al titular acceder a sus datos.

4.11 Realidad Actual

La globalización en el ámbito de la tecnología ha propiciado un entorno que constantemente evoluciona, por lo tanto, la protección de datos personales y la seguridad de la información se ha convertido en un tema relevante.

La reciente publicación, en fecha 26 de mayo de 2021 de la Ley Orgánica de Protección de datos Personales, implica el hecho de que aún no existan casos en los cuales las empresas se vean afectadas por el escaso desarrollo normativo y jurisprudencial en la materia, a comparación de otros países como España o México, incluso, grandes potencias como Estados Unidos, o Europa en General, los cuales cuentan con leyes, reglamentos y un amplio estudio de la temática, así como el ente autónomo que expide las directrices y guías tanto para responsables, como para titulares.

Es cierto que la LOPDP cuenta con el principio de responsabilidad proactiva para que los responsables (las empresas) puedan voluntariamente acogerse a códigos de protección que certifiquen que cumplen debidamente con la norma, pero, esto implicaría gastos adicionales debido a que deberían emplear costosas medidas como certificaciones o sellos que expresa la Ley.

Es en este contexto dentro del cual se desarrolla el presente trabajo investigativo, debido a que muchas empresas no cuentan con los recursos necesarios para adoptar las medidas de seguridad adaptadas a su giro de negocio que exige la Ley; la falta de un reglamento a la LOPDP son situaciones que propiciarán que las empresas incurran en algunas de las infracciones que

establece la norma, generando sanciones de carácter económico, causando grandes pérdidas, y no solo eso, las sanciones administrativas a los responsables, quienes, a falta de un buen desarrollo normativo en la materia, faltando un mes para la entrada en vigor de las medidas correctivas, no cuentan con la Autoridad de Datos Personales a la cual puedan acudir de ser necesario.

4.12 Marco Jurídico

El marco legal detallamos los siguientes artículos para postreramente hacer su debido análisis de cada uno de ellos.

4.12.1 Constitución de la Republica del Ecuador

La CRE (2008) fue el primer cuerpo legal en nuestro país en reconocer y garantizar como derecho constitucional la protección de datos personales, esto dentro de los derechos de libertad previstos en el artículo 66 numeral 19 de la Carta Magna.

Además de tutelar el mencionado derecho, la CRE también establece una vía constitucional para accionar el derecho a la protección de datos personales, esto es a través de la garantía jurisdiccional de Habeas Data, previsto en el art. 92 de la norma suprema. El Habeas Data ampara al titular para que este pueda "conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos" (Asamblea Nacional del Ecuador, 2008).

Se entiende entonces que la garantía constitucional del hábeas data tiene como propósito proteger y garantizar en todas sus dimensiones la protección de datos personales, que implicaría a su vez una protección al derecho a la intimidad, que en el caso de que llegase a ser vulnerado pueda tener graves afectaciones a el honor, buen nombre e integridad psicológica.

La Corte Constitucional manifiesta que:

> Viene a estar considerada como un mecanismo de satisfacción urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y advertirse sobre su finalidad, sea que dicha información conste en el registro o banco de datos público o privado. (Sentencia N.° 025-15-SEP-CC, 2015, pág. 11)

El acceso a los datos de carácter personal es un derecho, la normativa les otorga a los titulares la capacidad de acceder a ellos en cualquier momento, siempre y cuando exista una finalidad y manejo legal, y sean debidamente autorizados, cuando este derecho se ve obstaculizado es cuando el hábeas data funciona como un mecanismo rápido y eficaz para reparar esta vulneración.

4.12.2 Ley Orgánica de Protección de Datos Personales

A lo largo del trabajo investigativo, la principal fuente de análisis ha sido la "Ley Orgánica de Protección de Datos Personales", pues esta normativa representa el primer paso de Ecuador hacia la regulación de las nuevas tecnologías. Por ello es importante realizar un análisis y un estudio de la ley para conocer las obligaciones que tiene las empresas para con los titulares. Por lo tanto, uno de los artículos primordiales que prevé la ley es el artículo 4 referente a términos que nos permiten entender el denominado "sistema de protección de datos personales" con definiciones a conceptos muy utilizados en la práctica jurídica, los cuales fueron analizados en el marco contextual de la presente investigación.

Entre los artículos de interés para las compañías o responsables están: el artículo 7 referente al tratamiento legítimo de datos personas, el cual establece los parámetros para considerar "legítimo y licito un tratamiento", considera que se estamos ante un tratamiento legítimo e ilícito cuando se cumplen con uno o mas de los siguientes supuestos:

- Consentimiento del titular

- Cumplimiento de contrato o medidas precontractuales
- Obligación legal
- Orden judicial
- Intereses vitales
- Interés público
- Interés legítimo
- Información de acceso público

Como se puede observar, el tratamiento de datos personales es complejo, por lo cual, de no cumplirse con las condiciones antes expuestas, se estaría incurriendo en una infracción. El consentimiento del titular permite que el agente esté exento de responsabilidad; cuando se trate de un cumplimiento de contrato o medidas precontractuales, el responsable del tratamiento y el titular deberán haber suscrito un contrato el cual conlleve el tratamiento de datos personales, siempre y cuando se limite a lo estrictamente necesario, por su parte, de tratarse de medidas precontractuales, que obligan al tratamiento de datos personales, estas deberán ser a petición del interesado, mas no del responsable; el cumplimiento de una obligación legal, hace referencia a que el tratamiento de datos personales se puede amparar en el cumplimiento de una norma, ley, decreto, etc., la misma que establecerá la finalidad del tratamiento, así como prever otras especificaciones; los datos personales también pueden ser tratados en cumplimiento de una orden judicial, siempre y cuando se respeten los principios de la Ley; interés vital hace referencia a "situaciones de emergencia en las que peligra la vida de una persona, o como mínimo, a amenazas que supongan un riesgo de lesiones u otro daño para la salud del interesado o de otra persona" (Casal Tavasci, pág. 1), entonces el interés vital como base legal para el tratamiento de datos personales, debe ser usado cuando no pueda sustentarse en una base jurídica diferente, podríamos

decir que se trata de un último recurso; el interés legítimo, se relaciona con el consentimiento, puesto que, para tratar los datos personales, el responsable debe haber recabado el consentimiento del interesado, cabe desatacar que la satisfacción de un interés legítimo no prevalecerá sobre derechos o libertades fundamentales.

En cuanto a las obligaciones de los responsables estas se encuentran enumeradas en el artículo 47 de la LOPD, y desarrolladas en el marco teórico del presente trabajo. De la misma manera, para los casos de incumplimiento a las obligaciones por parte de los responsables, en el art. 65 se señalan las medidas correctivas, y en artículos posteriores (artículos 71 y 72) las sanciones.

4.12.3 Reglamento General de Protección de Datos

El RGPD es considerado uno de los ejemplares normativos mejor desarrollados en protección de datos personales, pues muchos de los preceptos establecidos en nuestra ley mantienen la misma línea que el RGPD. Entre los artículos que podemos mencionar están el articulado referente a los términos, a obligaciones de los responsables, a la protección de datos desde el diseño y por defecto, sanciones, entre otros (Reglamento General de Protección de Datos, 2016).

Este reglamento es "una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica" (Comisión Europea, como se citó en UNIR). Nos encontramos en una nueva era, la Era Digital, la cual gira en torno a nuevas tecnologías e internet, provocando cambios a la sociedad que se mueve ya en un mundo globalizado, esta era se ha manifestado a través de una gran revolución tecnológica, el internet, dispositivos tecnológicos, herramientas digitales y demás, son parte de ello, estamos hablando de que se ha ofertado una gran ventaja a la sociedad, pero como todo, presenta algunos

inconvenientes, y es que, ahora la información, que antiguamente constaba solo en papel, se encuentra digitalizada, ello no significa que sea invulnerable, al contrario, es susceptible de ataques. Es por ello, que surgió la necesidad de proteger los datos de las personas, (que como ya se había manifestado, es un derecho) por lo tanto, el RGPD surgió como un medio idóneo de respetar los derechos de las personas titulares de datos.

4.12.4 Derecho Comparado

4.11.4.1 España y los datos personales

La Constitución Española de 1978, publicada en el Boletín Oficial del Estado de 29 de diciembre de 1978, en su Artículo 18 consta el Derecho al honor, a la intimidad personal y familiar, a la inviolabilidad de domicilio y secreto de las comunicaciones. Los Derechos Fundamentales Garantiza la Constitución Española en uno de los incisos del Artículo 18, numeral 4, señala. “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (Las Cortes , 2011, pág. 12).

La preocupación del legislador era la de proteger a las personas frente a los avances tecnológicos, entre estos tenían presente la computadora, al alcance del público. La posibilidad de que los seres humanos tengan acceso de una herramienta con capacidad de cálculo y almacenamiento de información, fue donde el legislador tuvo el interés de incorporar en uno de su texto Constitucional la limitación de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En la legislación interna, se llevó a cabo por medio de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, en cuya exposición de motivos manifiesta que:

"(…) desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida" (Cortes Generales, 1992, pág. 1). Como se puede evidenciar, uno de los principales motivos por los cuales se regula la protección de datos personales en España es el avance y desarrollo tecnológico, por lo tanto "la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo" (Cortes Generales, 1992, pág. 1). Los Datos personales son un tópico de gran relevancia, pues se trata de nuestra identidad como persona, de toda aquella información que nos identifica como tal, por lo tanto, el mal uso de ella nos compromete, entonces una rigurosa protección legal es completamente necesaria.

La Ley maneja los principios de autodeterminación y consentimiento, siendo este último uno de los ejes sobre el cual gira nuestra Ley Orgánica de Protección de Datos Personales, no es de extrañar, puesto que el Reglamento General expedido por el parlamento Europeo se maneja en similar medida.

Respecto del Objeto de la Ley Orgánica de Protección de Datos el artículo 1 manifiesta que, tiene por objeto "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos." (Cortes Generales, 1992, pág. 3). La Ley española considera una medida de seguridad general, el limitar el uso de la informática, esto debido a que es mediante ella que se producen graves afectaciones a los datos de las personas. El objeto de esta ley, es un tanto diferente a la nuestra, pues mientras la LOPDP ecuatoriana tiene como objeto principal el garantizar el ejercicio del derecho a la protección de datos personales, la ley española prevé la limitación de el uso de medios informáticos para garantiza efectivamente esos derechos.

Respecto de la Autoridad de Protección de Datos Personales, en España la encargada es la Agencia de Protección de Datos, la cual tiene la función de hacer cumplir con lo dispuesto en la Ley, entre otras funciones establecidas en el artículo 36.

4.12.4.2 Protección de datos personales en México

Gracias a los avances tecnológicos y la sociedad de la información, en México nace la necesidad de salvaguardar sus datos, es así que pertenece a la Red Iberoamericana de Protección de Datos. Establecida en el año 2013 por países iberoamericanos cuya finalidad es la de defender la cultura de privacidad en todos los países, la de favorecer la legislaciones y jurisprudencias a las personas, de la misma manera dar a conocer sus derechos entre ellos existentes, promoviendo una seguridad en la protección de datos personales. Frente a este gran paso que ha dado el país mexicano, se dice que reconoce la importancia de la protección de datos personales y la ley que debe regular este derecho. En la Constitución los Estados Unidos Mexicanos en su Artículo. 16 nos dice:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Congreso Constituyente de México, 1917, pág. 17)

En la Constitución de los Estados Unidos Mexicanos también hace referencia al derecho que tiene la persona, es decir el de acceso, rectificación, cancelación y oposición de sus datos cuando el titular así lo vea conveniente. Conocidos también como el derecho ARCO. Es necesario indicar una de las leyes que protege la información y protección de datos. La protección de datos

en los estados Unidos Mexicanos lo detallas de manera más clara a los organismos públicos, es decir cuando nuestra información personal se encuentra en manos de entidades públicas o privadas esta ley garantiza su acceso, haciendo mención a uno de los principios básicos que se encuentra en la Ley Federal de Protección de Datos en Poder de Particulares. El Instituto Federal de Acceso a la Información y Protección de Datos Personales. (IFAI) 2011. Es el encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de dependencias y entidades. Es por esa razón que: En la (Constitución de los Estados Unidos Mexicanos, 5 de febrero de 1917) en su Artículo 6. Numeral VIII. Dice: La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley. El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal.

Es necesario indicar una de las leyes que protege la información y protección de datos. La protección de datos en los estados Unidos Mexicanos lo detallas de manera más clara a los organismos públicos, es decir cuando nuestra información personal se encuentra en manos de entidades públicas o privadas esta ley garantiza su acceso, haciendo mención a uno de los

principios básicos que se encuentra en la Ley Federal de Protección de Datos en Poder de Particulares. El Instituto Federal de Acceso a la Información y Protección de Datos Personales. (IFAI) 2011. Es el encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de dependencias y entidades. Es por esa razón que: En la (Constitución de los Estados Unidos Mexicanos, 5 de febrero de 1917) en su Artículo 6. Numeral VIII. Dice: La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley. El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal.

Instituto Federal de Acceso a la Información y Protección de Datos Personales- (IFAI). El organismo es encargado, fundamentalmente, de: 1. Garantizar el derecho de acceso de las personas a la información pública gubernamental. 2. Proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares. 3. Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

Calidad de los datos

- El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea. (Reglamento Protección de Datos Personales, 2016). Artículo 36

(LFPDPPP) Ley Federal de Protección de Datos Personales en Posesión de Particulares Para la protección de los datos personales México cuenta con una ley para la protección de los mismos, conocido como Ley Federal de Protección de Datos Personales en Posesión de Particulares. Ante esta iniciativa podemos indicar de qué manera protegen sus datos en este país como es México. La (Ley Federal de Protección de Datos en Poder de Particulares - LFPDPP, 2010). Artículo 1. Objetivo. "Tiene como objetivo proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

4.12.4.3 Protección de Datos en Reino Unido

La Ley de Protección de Datos de Reino Unido (*Data Protection Act*) otorga a las personas el derecho a acceder a sus propios datos personales a través de solicitudes de acceso de sujetos y contiene reglas que deben seguirse cuando se procesan datos personales. La Ley funciona de dos maneras: a) proporciona a las personas derechos, incluido el derecho a saber qué información se tiene sobre ellos y el derecho a acceder a esa información; y, b) establece que cualquier persona que procese información personal debe cumplir con los principios de la Ley.

Cabe destacar, que la Ley de Protección de Datos se complementa con el Reglamento General de Protección de Datos (*General Data Protection Regulation*). El RGPD del Reino Unido y la Ley se aplican al procesamiento de datos personales por parte de los controladores o procesadores.

Según el GDPR y el DPA ““Personal data” means any information relating to an identified or identifiable living individual” (Queen’s most Excellent Majesty, Lords Spiritual and Temporal, Commons, & Parliament, 2018). Es decir, datos personales son información relacionada con una persona viva identificada o identificable, por lo tanto, el marco de protección de datos no se aplica a la información relacionada con personas fallecidas, ni cubre el procesamiento de información que concierne a personas jurídicas (como empresas). Estos asuntos quedan fuera del alcance del RGPD y la Ley del Reino Unido.

Por su parte, respecto de la Autoridad en materia de protección de datos personales, el encargado es “The Commissioner” o el Comisionado, cumple esta función el ICO (*Information Comissioner’s Office*) Los principales deberes del ICO son monitorear y hacer cumplir el RGPD del Reino Unido, incluido el manejo de quejas de los interesados y la realización de investigaciones, así lo establece el artículo 57 “Sin perjuicio de otras funciones previstas en el presente Reglamento, el Comisario deberá: (a) monitorear y hacer cumplir la aplicación de este Reglamento” (Parlamento Europeo, 2016, pág. 57). También se le confía la responsabilidad de proporcionar asesoramiento a los controladores y procesadores cuando sea necesario (por ejemplo, en virtud del artículo 36 cuando se requiere una consulta con el ICO en relación con una Evaluación de impacto de la protección de datos ('DPIA')) y de promulgar ciertas guías y documentos, tales como códigos de conducta y Cláusulas contractuales estándar ('SCC'). Los poderes de investigación del ICO son amplios e incluyen el poder de realizar una auditoría a un controlador o procesador, registrar locales, emitir advertencias, amonestaciones y multas, imponer limitaciones y prohibiciones en el procesamiento, suspender flujos internacionales de datos y exigir la realización de determinadas comunicaciones a los interesados. El ICO también tiene

poderes de asesoramiento y autorización y puede aprobar (por ejemplo) salvaguardas para transferencias internacionales de datos, como las Normas Corporativas Vinculantes ('BCR').

La Ley complementa las tareas y poderes que se establecen en el RGPD del Reino Unido, de la siguiente manera:

- La Parte 5 de la Ley contiene otras disposiciones específicas que complementan los deberes y facultades de la ICO, incluidas las salvaguardias impuestas en el ejercicio de las facultades de la ICO; y
- La Parte 6 de la Ley establece los poderes de ejecución de la ICO en detalle, incluidos los poderes para imponer avisos de información, avisos de evaluación, avisos de ejecución y sanción, así como poderes de entrada e inspección, y los delitos penales específicos que el ICO tiene poder. para procesar en el Reino Unido.

El ICO está obligado a llevar a cabo sus tareas y ejercer sus poderes con total independencia (artículo 52 del RGPD del Reino Unido).

Como se puede evidenciar, en Reino Unido, la protección de datos personales está regulada por una Ley y por el Reglamento, por lo tanto, es un derecho que cuenta con un fuerte amparo legal, justificado completamente por la importancia del mismo, además, la existencia de la Autoridad de Protección de Datos, es muy importante para asegurar el cumplimiento de la normativa.

Es evidente que nuestro país, va muy atrás en cuanto a esta materia, sin Autoridad, sin Reglamento, no se puede pretender una correcta aplicación de la Ley.

5. Metodología

5. 1 Materiales utilizados

Los materiales utilizados para el presente proyecto de investigación fueron libros jurídicos de diferentes autores, artículos científicos, revistas, sentencias, páginas web; de lo mencionado tenemos citado al final del presente proyecto de investigación.

Entre otros materiales que fueron de gran ayuda se emplearon: celular portátil, cuaderno, esferos, fotocopias, impresiones, internet, anillados, empastados, etc.

5.2 Métodos

Por métodos debemos entender que es una forma organizada y sistemática para poder alcanzar un objetivo determinado y facilitan con el desarrollo de la investigación entre estos métodos tenemos:

Método Inductivo: Según opinión general, se define al método inductivo como el procedimiento lógico que de lo particular lleva a lo universal. Este método fue aplicado en la presente investigación en el marco teórico, en donde se dieron a conocer conceptos básicos relacionados al ámbito de datos personales, hasta un análisis de los sujetos intervinientes y su función en el manejo de información.

Método Deductivo: Se lo entiende como un proceso del pensamiento en el que, de afirmaciones generales, se llegaba a afirmaciones particulares. Este método fue utilizado en el apartado de marco teórico del presente trabajo investigativo, en donde se estudió todo aquello relacionado con las medidas de seguridad, hasta llegar a establecer cuáles serían las consecuencias que establece la LOPDP en el caso de que las empresas no las implementen y apliquen.

Método Analítico: El método analítico es aquel método de investigación que consiste en la desmembración de un todo descomponiéndolo en sus partes o elementos para observar las

causas, naturaleza y los efectos. Muestra de ello es el estudio de las medidas de seguridad y los distintos tipos que existen y se pueden aplicar en las empresas.

Método Exegético: Con este método se realizará un estudio minucioso con la finalidad en las normas jurídicas el significado que el legislador le dio a dicha norma, en el presente trabajo de titulación fue utilizado en las normas inherentes al tópico de mi investigación: Constitución de la República del Ecuador, Ley Orgánica de Protección de Datos Personales; Reglamento General de Protección de Datos Personales (Parlamento Europeo).

Método Sintético: El método sintético es un proceso de análisis de razonamiento que busca la forma de reconstruir un acontecimiento de manera resumida, valiéndose de los diferentes elementos fundamentales que estuvieron presentes en el desarrollo del acontecimiento, este método fue empleado en la parte final del presente trabajo de titulación en la verificación de objetivos, la fundamentación legal de la propuesta jurídica, así como la contrastación de hipótesis.

Método Histórico: Método empleado al momento de realizar un recuento histórico de las diferentes etapas que ha tenido nuestra legislación en cuanto a protección de datos personales se refiere.

Método Comparativo: Este método permite contrastar dos realidades legales. Es decir que esta comparación se la puede realizar a través de normas nacionales con otras extranjeras, este método fue aplicado en el apartado de Derecho Comparado, en donde se estudió como en las legislaciones, mexicana, española e inglesa manejan la protección de datos personales.

5.3 Técnicas

Encuesta: La encuesta como técnica de investigación se caracteriza por utilizar una serie de procedimientos estandarizados, a partir de cuya aplicación se recogen, procesan y analizan un

conjunto de datos de una muestra, correspondientes al tema de investigación el cual no llevara al objetivo de estudio que se ha planteado.

Entrevista: La entrevista consiste en un conjunto de preguntas, normalmente de varios tipos, preparado sistemática y cuidadosamente, sobre los hechos y aspectos que interesan en una investigación o evaluación, para después proceder con un análisis concreto sobre cada pregunta y respuesta que será valorada en un análisis detallado para asumirlas dentro de mi trabajo de titulación.

6. Resultados

6.1 Tabulación y Análisis de resultados de encuestas

En el siguiente apartado se realizará un análisis descriptivo estadístico respecto de los resultados obtenidos a través de la técnica de encuesta. La muestra a la cual se aplicó la técnica en mención fueron treinta profesionales del Derecho a quienes se les consulto de 5 preguntas que son relacionadas que son relacionadas con el objeto de investigación, cuya interpretación y análisis se realizará a continuación:

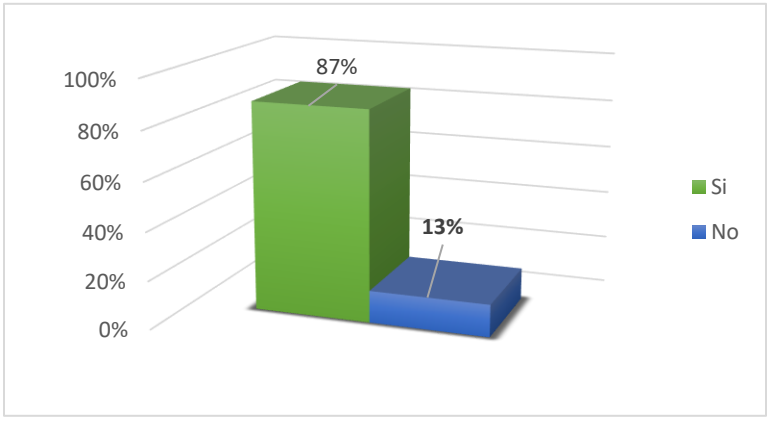
Primera Pregunta: ¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?

Tabla 2. Cuadro Estadístico Nro. 1

Indicadores	Frecuencia	%
Si	26	87%
No	4	13%
Total:	30	100%

Fuente: Profesionales del Derecho de Loja.
Autor: Lady Carolina Pardo Guamán

Figura 2. Representación Gráfica Nro. 1



Interpretación:

Del cuadro y gráfica anteriormente mostrados, se puede evidenciar que veintiséis profesionales del Derecho correspondientes al ochenta y siete por ciento de la población, respondieron que efectivamente conocen la nueva LOPDP; por su parte, cuatro profesionales del Derecho, correspondientes al trece por ciento de la población encuestada manifestaron desconocer.

Análisis:

Gran parte de los profesionales del Derecho encuestados afirman conocer la Nueva Ley Orgánica de Protección de Datos Personales, no es de extrañarse, puesto que la misma fue un gran avance en esta materia. La Protección de Datos Personales, surge como un mecanismo para proteger el derecho a la vida privada a partir de finales de los años 1970 en países europeos como Francia y Alemania. La Unión Europea se convirtió en el ejemplo a seguir en el área a partir de la directiva 95/46/CE, la falta de homogenización y mecanismos capaces de asegurar su cumplimiento provocaron la promulgación de el Reglamento General de Protección de Datos Personales, el cual, en muchos países ha sido tomado como guía para la expedición de diversos cuerpos normativos. Ecuador no se quedó atrás, y en mayo del 2021 se dio un gran paso en nuestra legislación, la cual, en pro de adaptarse a la era digital, aprobó la tan necesaria LPDP. A criterio

de los abogados encuestados, es una ley que carece de claridad en determinadas temáticas, pero, reconocen es un buen inicio para que procure un adecuado desarrollo normativo.

Por su parte, es desconcertante que algunos profesionales desconozcan este cuerpo legal, como miembros parte de este sistema de justicia, ¿cómo es posible que no estén enterados de la promulgación de esta Ley? A la par que la tecnología ha ido avanzando, los esfuerzos por adaptarse a ello deben ser obligatorios para todos, el uso de las Tecnologías de Información y Comunicación debe ser regulado, y esta norma debe ser de conocimiento general.

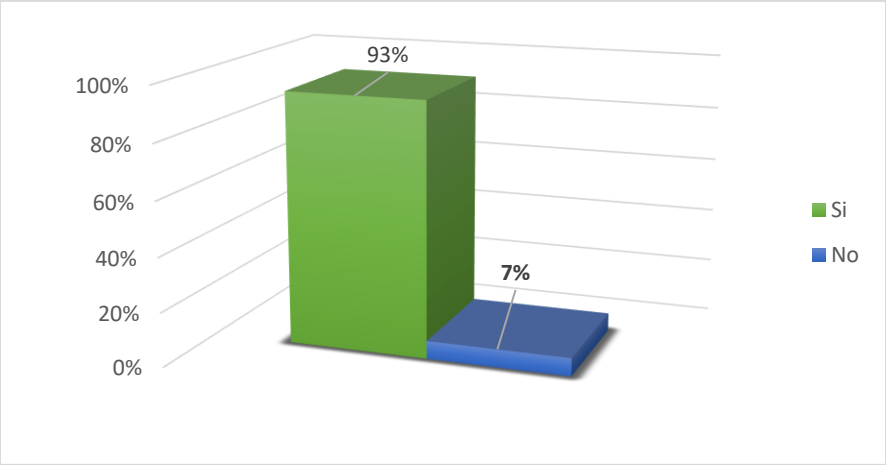
Segunda Pregunta: ¿Conoce usted acerca de las medidas de seguridad que deben implementar las empresas, así como las obligaciones que deben en su calidad de responsables, para garantizar la protección de datos personales?

Tabla 3. Cuadro Estadístico Nro. 2

Indicadores	Frecuencia	%
Si	28	93%
No	2	7%
Total:	30	100%

Fuente: Profesionales del Derecho de Loja.
Autor: Lady Carolina Pardo Guamán

Figura 3. Representación Gráfica Nro. 2



Interpretación:

De la tabla y gráfica anteriores se desprende que veintiocho profesionales del Derecho expresaron conocer las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales, correspondiendo ello al noventa y tres por ciento de la población total encuestada; por su parte, dos profesionales del Derecho afirmaron desconocer las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales, siendo parte del siete por ciento de la población encuestada.

Análisis:

La mayoría de los profesionales del Derecho encuestados aseguran conocer las obligaciones inherentes a las empresas en materia de protección de Datos Personales, y, no es extraño, dado que a pesar de que puedan desconocer la LOPDP, las obligaciones que tienen las empresas para con la seguridad de los datos de los titulares, ya fueron establecidas en el Reglamento General de Protección de Datos emitido por la Unión Europea, que fue un precedente clave para demás legislaciones en distintos países. Las obligaciones de las empresas en la práctica implican que deban cumplirlas, puesto que, como mínimo, tratarán los datos personales de sus empleados. Independientemente de si es una empresa de marketing, un restaurante, un centro educativo, un centro sanitario, una gestoría, un medio de comunicación, una tienda online o un despacho de abogados, las obligaciones de protección de datos no son una excepción para ninguna de ellas.

Del mismo modo, afirman conocer respecto de las medidas de seguridad que menciona la Ley, pero dentro de sus motivaciones, establecen que si bien es cierto, la norma menciona algunas medidas de seguridad, no las conceptualiza de manera debida y mucho menos en que casos se debería aplicar, es por ello, que consideran pertinente la emisión de un reglamento en la materia.

Criterio con el que esta autora está completamente de acuerdo, la falta de una norma reguladora a la Ley principal podría tener como consecuencia que las empresas incurran en infracciones, lo cual provocará que sean sancionadas por no haber aplicado correctamente la Ley, ya sea porque la ignoraron o simplemente porque no tenían plena certeza de la correcta aplicabilidad.

Una minoría afirma desconocer las obligaciones de las empresas en materia de protección de datos, lo cual da a denotar un desinterés de algunos profesionales del Derecho en algo tan importante en la actualidad.

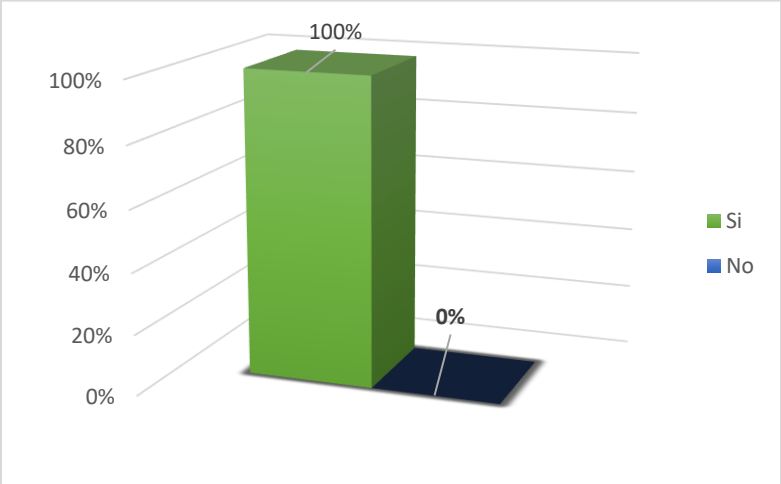
Tercera Pregunta: La LOPDP establece un régimen sancionatorio para aquellas empresas que no se acoplen a lo establecido en el texto legal ¿tiene usted conocimiento acerca de dicho régimen?

Tabla 4. Cuadro Estadístico Nro. 3

Indicadores	Frecuencia	%
Si	30	100%
No	0	0%
Total:	30	100%

Fuente: Profesionales del Derecho de Loja.
Autor: Lady Carolina Pardo Guamán

Figura 4. Representación Gráfica Nro. 3



Interpretación:

De la tabla y gráfico anteriores se puede evidenciar que treinta profesionales del derecho, correspondientes al cien por ciento de la población encuestada, afirman conocer el régimen sancionatorio de la Ley Orgánica de Protección de Datos Personales

Análisis:

En consonancia con la anterior pregunta, la totalidad de profesionales del Derecho encuestados afirman conocer el régimen sancionatorio que establece la LOPDP, evidenciando su parecido con el Reglamento General Europeo, manifiestan también, que para que este régimen sancionatorio pueda tener la eficacia necesaria, es pertinente que se desarrolle un reglamento a la Ley, puesto que, hay situaciones que deberían estar establecidas de forma clara, evitando así que las empresas incurran masivamente en infracciones que conlleven la aplicación de este régimen sancionatorio.

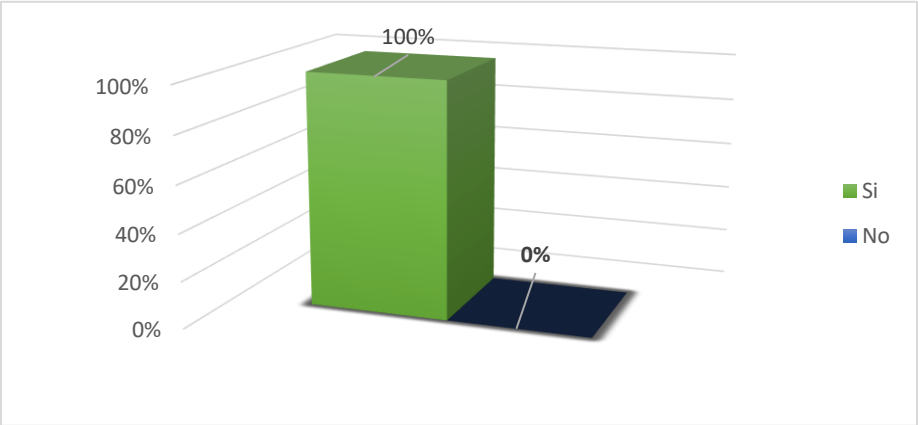
Cuarta Pregunta: A su criterio ¿Considera que las empresas se verían afectadas una vez entrasen en vigencia las medidas correctivas debido a la falta de un reglamento a la LOPDP, así como la inexistencia de la Autoridad pertinente?

Tabla 5. Cuadro Estadístico Nro. 4

Indicadores	Frecuencia	%
Si	30	100%
No	0	0%
Total:	30	100%

Fuente: Profesionales del Derecho de Loja.
Autor: Lady Carolina Pardo Guamán

Figura 5. Representación Gráfica Nro. 4



Interpretación:

De la tabla y gráficos anteriores, se desprende que treinta profesionales del Derecho manifestaron que las empresas se verían afectadas una vez entrasen en vigencia las medidas correctivas debido a la falta de un reglamento a la LOPDP, así como la inexistencia de la Autoridad pertinente, correspondiendo ello al cien por ciento de la población encuestada.

Análisis:

La totalidad de los profesionales encuestados afirman que las empresas se verían afectadas una vez entrasen en vigencia las medidas correctivas, por dos circunstancias: debido a la falta de un reglamento a la LOPDP, y es que, la LOPDP en el tema de medidas de seguridad es demasiado amplia, no especifica de forma clara cuales son y las circunstancias en las cuales se pueden aplicar, esta autora entiende el concepto de que deben adaptarse a su giro de negocio y actividades en general que desempeñen, no es suficiente, es completamente necesario un reglamento; además, hasta el momento aún no se ha designado a la Autoridad de Control ni se ha creado la Superintendencia de Protección de Datos, lo que significa que no se ha podido proporcionar los recursos y medios necesarios para su correcta aplicación según lo establecido por la ley

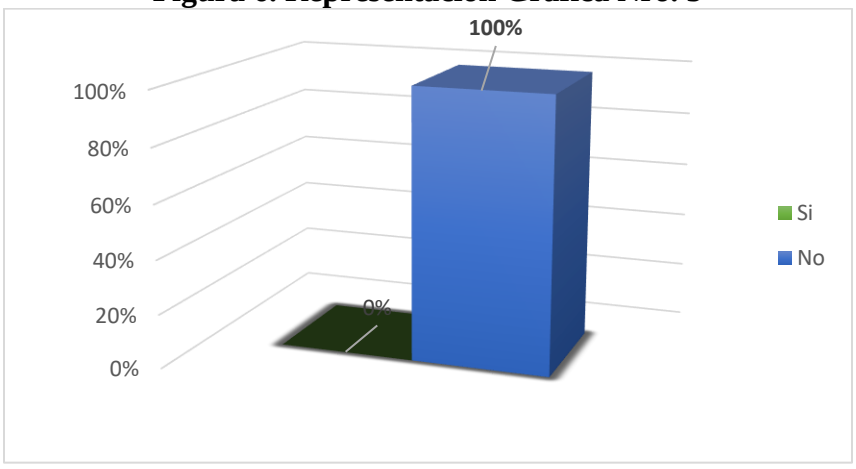
Quinta Pregunta: ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

Tabla 6. Cuadro Estadístico Nro. 5

Indicadores	Frecuencia	%
Si	0	0%
No	30	100%
Total:	30	100%

Fuente: Profesionales del Derecho de Loja.
Autor: Lady Carolina Pardo Guamán

Figura 6. Representación Gráfica Nro. 5



Interpretación:

Del cuadro estadístico y gráfica anteriormente detalladas se obtiene que veintiocho profesionales del Derecho consideran que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es insuficiente, correspondiente ello al noventa y tres por ciento de la población encuestada; por su parte, dos profesionales del Derecho, manifestaron su conformidad con el tiempo establecido en la norma, correspondiendo al dos por ciento de la población encuestada.

Análisis:

Por último, la totalidad de los profesionales encuestados afirman que el tiempo establecido para que empiece a operar el régimen sancionatorio es inadecuado, concordando plenamente con el tema principal de la presente investigación. No es sencillo para las empresas adaptarse a la nueva Ley puesto que cada sector u organización tiene necesidades diferentes y responde a realidades distintas; no hay recetas únicas ni estandarizadas. "Un proceso de adaptación implica cumplir con dos etapas: Diagnóstico situacional del nivel de cumplimiento de la organización a la Ley de Protección de Datos Personales; e, Implementación de las medidas que se deben adoptar para el cumplimiento de la norma" (PRIMICIAS, 2023). Constituye esto una gran responsabilidad de las empresas, siendo necesarias grandes inversiones que en algunos casos no están listos para asumir. Además, la falta de supervisión por parte de estas autoridades inexistentes impide que la Ley de Protección de Datos Personales (LOPDP) sea aplicada adecuadamente.

6.2 Resultados De Las Entrevistas

Entrevistas realizadas a profesionales especialistas en la materia

Entrevistado Nro. 1:

Pregunta nro. 1: ¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?

Si. La ley fue publicada el 23 de mayo del 2021, y establece un sistema de protección de datos personales en el régimen ecuatoriano. Se basa en el reconocimiento del derecho fundamental de la protección de datos personales como dice el objeto de la ley, el propósito que tiene el artículo 1 dice que es justamente desarrollar este derecho estableciendo mecanismo de tutela, principios, obligaciones. La ley en su articulado reconoce trece principios, mucho de ellos parecidos a los del Reglamento Europeo de Protección de Datos, realmente la ley es muy similar basada y casi copiada y se nota en algunas partes del articulado. Lo que más resalta de la ley es su approach semejante

al del (RGDP) eso quiere decir que la normativa procura derivadamente ser flexible, amplia, ambigua porque establece las obligaciones a las entidades en función de riesgo es decir les obliga a que hagan un análisis de riesgo para establecer medidas de mitigación de ese riesgo, eso es un proceso de gestión de riesgo, entonces a lo largo de la normativa vamos a encontrarnos

Esas estipulaciones de gestionar el riesgo y este pues la aproximación que tiene el Reglamento Europeo, también a mayor riesgo de tratamiento y también establece mayores requerimientos. Es cierto que les deja a los privados escoger la medida pero también cuando por defecto la ley quiere poner ciertos requerimientos es porque considera que determinadas actividades de tratamiento son más riesgosas, es por eso que establece cierto mecanismo, por ejemplo: en la evaluación de impacto de tratamiento que es una obligación reforzada y adicionalmente un principio importante como es el principio de responsabilidad proactiva y demostrada, basado en la responsabilidad, el RGDP también lo tiene, es importante porque establece para los responsables del tratamiento que ellos deben ir más allá de los mínimos y además estar en capacidad de demostrar que están cumpliendo, eso debería traducirse a nivel regulatorio en una approach de la autoridad de protección de datos personales que sea de controles. El principio de la responsabilidad deliberadamente fue desarrollado en Europa con el propósito explícito de reducir las cargas administrativas de las autoridades. En el artículo 29 ahí tú puedes encontrar como están estructurados estos principios y también como se traducen a nivel de controles que tienen esos principios tienes una serie de derechos muy parecidos a los del RGPD pero no equivalentes ni iguales, tienes un régimen ordinario de base de tratamiento de datos que están en el artículo 7 que reconoce ocho bases donde tienes un régimen diferente para el tratamiento de datos que sensibles que está descrito en el artículo 26 y en el 29, 30 y 31 qué son los datos relativos de la salud muy semejantes, pero no equivalente al efecto. Hay varios puntos

diferentes pues tienes también una parte de seguridad de la información que te está pidiendo que la apliques medidas de seguridad, tienes una autoridad que tiene potestad sancionadora, tienes medidas correctivas, tienes diferentes actores entre ellos una figura importante que es el delegado de Protección de Datos personales, además de los roles de responsable y encargado, y en otros temas que están en la ley; en todo caso conozco la norma a detalle, la he estudiado y la manejo en la práctica para clientes nacionales extranjeros con operación nacional como operación multinacional y también a nivel académico estoy incluido generando material para la academia y también para las entrevistas especializadas

Pregunta Nro. 2: ¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales?

Sí, están descritas en 14 numerales en el artículo 47 de la ley, simplemente es como la columna vertebral y es muy general. Establece obligaciones muy específicas como por ejemplo la suscripción de contratos de tratamiento adecuado de datos tanto con los encargados con los colaboradores porque ahí se implementen mecanismos de gestión de riesgo adecuados que las que se implemente mecanismos de monitoreo y mejora continua de estas herramientas para mi mitigar el riesgo y varias cosas más.

Son 14 numerales si no estoy mal, no son exhaustivas al final tiene una cláusula abierta que te dice “y las demás de esta ley y la normativa aplicable” entonces, las conozco las partes que bueno tienes la obligación relativa a atender y garantizar los derechos de los titulares, tienes la de procesamiento legítimo que es bueno estructurar la base de la legitimidad, tienes la seguridad del dato personal se refiere específicamente a la disponibilidad, confidencialidad, integridad del dato personal y pues por allí ya están algunas otras. Algunas obligaciones adicionales pueden ser la

evaluación de impacto del tratamiento en determinados contextos específicos también puedes interpretar a los principios como obligaciones, teniendo en cuenta que son parámetros de optimización que deben observar en todo momento los responsables del tratamiento. Conozco la normativa tanto en abstracto y en como traducirlas en la práctica a conductas auditables, medidas concretas, para eso puede servir mucho la norma ISO 27701 que toma los controles de la ISO 27001 que es la especialidad en sistema de gestión de la seguridad de la información, toma esos controles los extiende y agrega controles específicos para el rol de responsable y de encargado del tratamiento. Ya en la práctica este tipo de herramientas y este marco de referencia, aun cuando la empresa no quiere implementar un sistema de gestión puede pueden ser de gran ayuda para traducir la norma a la práctica.

Pregunta Nro. 3: A su criterio ¿Cuáles son los retos que genera la implementación de la Ley Orgánica de Protección de Datos Personales dentro de los procesos internos de las empresas?

Por un lado, tienes la falta de talento capacitado, por otro lado, tienes la falta de madurez digital y la falta de madurez en sistemas de cumplimiento de las empresas (eso no suele pasar en sectores hiper regulados), en sectores que tengan sistemas de gestión de la calidad o algún sistema de gestión de las normas de ISO o alguna otra norma estandarizada semejante, entonces tú tienes un primer desafío de cultura interna y de compromiso corporativo con el cumplimiento. Tienes también una escasez de este de talento porque la seguridad de la información tiene overlap los protección de datos personales pero no es por sí sola suficiente ni tampoco tiene el mismo enfoque, de hecho la seguridad de la información se enfoca en el riesgo que tienes tú de cara al negocio en el tema de la formación, pero en cambio la protección de los datos personales es el riesgo que corre el titular de los datos en cuanto a sus derechos y libertades por el tratamiento de los datos, entonces

en el caso de la de la gestión y Gobierno de Protección de Datos personales conviven dos enfoques de gestión del riesgo este que tiene en cuenta los objetivos de negocio de la empresa, qué riesgo hay si es que yo no cumpla normativa eso se les llama técnicamente riesgo legal de cumplimiento, y el riesgo que te que te manda a analizar la norma ecuatoriana que es el riesgo. Otro riesgo también es cierta incertidumbre regulatoria, aunque esto es un desafío, pero más porque la gente lo percibe así realmente como te dije al inicio la norma está deliberadamente hecha de forma muy general de modo que no va a haber mayor cambio de fondo en la normativa salvo un par de cosas más y como es una norma copia del RGDP podemos evitar mucho el retrabajo es decir volver a trabajar de gana, entonces muchas organizaciones se enfrentan a eso. Si quieres ser más concreta también algunos puntos de gestión y gobierno a quién le encargas tú la gobernanza de eso a la función de riesgo, a la función legal, a la función de seguridad información o constituyes un órgano colegiado cómo lo gestionas y lo gobiernas ese es otro punto importante. Otro punto como esa falta de experiencia en el sector, cómo empezamos, que debemos de hacer que evaluamos inclusive los que son técnicos en la parte segura en información no siempre tienen ven a ver bien los dominios porque como esto tiene que ver con una normativa, le digo yo desde mi experiencia personal cuando he trabajado conjuntamente con gente de seguridad de la información, levanta ciertos criterios que no necesariamente están adecuados a la normativa. Para temas de implementación algunos han confundido la evaluación de decir vamos a evaluar determinadas cosas de privacidad refiriéndose a Protección de Datos entonces ese nivel de sofisticación y a veces esto diría esos esos parámetros la parte de falta de talento, pero también la falta de madurez digital de las empresas y las incógnitas en cuanto a gestión y gobierno además de cómo empezar y cómo llevar procesos de implementación.

Pregunta Nro. 4: ¿Cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?

Si tú te fijas en las medidas correctivas están mal hechas, responden a una esquematización de infracciones graves, muy graves y leves; tratan de hacerse funcionales cuando se constituya la autoridad, pero si deja mucha incógnita.

En cuanto al régimen sancionatorio, es necesario como mecanismo de incentivo, no tengo ninguna opinión negativa respecto de eso, de hecho, las sanciones se hicieron más bajas de lo que estaban en durante el proceso legislativo, pues se estaba planteando una cuantía sumamente alta y durante el proceso legislativo, en las discusiones que en las que estuvimos, la asamblea se hizo tomar conciencia y se mitigó, pero en si es necesario ese régimen sancionatorio. Ahora tal vez podríamos decir más cosas cuando el régimen esté funcionando porque tú sabes necesitamos una construcción de una de normativa secundaria para poder operativizar eso.

Pregunta Nro. 5: ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

El tiempo realmente fue puesto a dedo, si tú estás al tanto de lo que pasó con el RGPD en 2016 y en 2018 entró en vigencia todo este tema y parece que se les ocurrió simplemente poner el mismo número. Es complicado porque como tú dices por un lado no hay autoridad, pero ha sido un tema coyuntural y político, que se sale del alcance del tema del legislativo, es un tema coyuntural eso quizá va un poquito más afuera de ese debate exclusivamente formalista que a veces se hace, pero en todo caso el tiempo si es insuficiente, pero se hizo insuficiente por tema político no por un tema técnico.

Desde un punto de vista de capacidades, de habilidades de las empresas sí que dejan mucho que desear porque tú te das cuenta de que nosotros estamos acelerando de cero a cien en muy poco tiempo. Si tú tomas en cuenta lo que pasó en Europa, no todas las empresas se lograron acomodar al RGPD y eso que tenían la directiva que estaba desde el año 1995 y leyes nacionales que las desarrollaban. Incluso hubo un estudio que hace referencia tangencial a una métrica específica de que varias empresas (un porcentaje alto) creía que iba a cumplir, pero a la hora de la hora muy pocos cumplieron.

Es un tiempo francamente insuficiente pero también es el dilema de que si hubiera sido más tiempo quizás las cosas se estarían relajando todavía más, entonces eso no podemos saber si es suficiente o insuficiente, en todo caso sabemos que nosotros no tenemos el nivel de madurez que tenía Europa y eso es un desafío grande que estamos experimentando. Si tú ves en Europa como el patrón de la cuantía de las sanciones del RGPD van subiendo en función de cuánto tiempo va pasando respecto del momento en que entró en vigencia, puede ser que algo semejante sucede aquí, tomando en cuenta que la responsabilidad te exige que hagas tú controles y que dejes mucho. Quizá va a suceder que la autoridad no va a ser tan agresiva al momento de entrar o puede ser como la Superintendencia del Control de Mercado que entró dando puños y patadas; en todo caso dependerá de la actitud que tenga la autoridad. Un caso muy interesante es la actitud que tienen autoridad mexicana que promueve mucho el cumplimiento y ayuda mucho a las empresas te recomendaría que te veas cómo está trabajando la autoridad mexicana es un referente bastante bueno. Si bien es insuficiente, la autoridad tendrá, si quiere hacer bien su trabajo, ayudar a las empresas sino simplemente podrá instrumentarse para fines recaudatorios, empezar a sancionar generalmente a los primeros que les caen son a los sectores y hiperegulados como telecomunicaciones, banca y demás.

Entrevistado Nro. 2:

Pregunta Nro. 1: ¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?

Si, la ley fue promulgada el 26 de mayo de 2021; para el giro del negocio que nosotros tenemos, en el que captamos y tratamos datos de manera masiva, estuvimos monitoreando desde el proyecto de ley, las reuniones, mesas de trabajo que se hicieron en la Asamblea previo a la promulgación de la Ley. Aún estamos a la espera del reglamento y la posición de la autoridad para adecuar los procesos que tenemos aquí en la compañía a la normativa, pero ya hemos empezado por una auditoria para la adecuación de ley en Cervecería Nacional y todas las empresas relacionadas; ya finalizamos una primera fase de ese proyecto que era un proceso de Auditoría Interna, levantamiento de información con unos consultores externos, levantamos todos nuestros procesos virtuales, recopilamos y tratamos datos personales, se nos presentaron recomendaciones preliminares en una forma de remedición y es lo que actualmente nos encontramos ejecutando para estar listo para el próximo año, porque en mayo del 2023 (a pesar de que no hay autoridad) ya habría la posibilidad de que existan sanciones para la compañía sino estamos adecuados a la ley.

Pregunta Nro. 2: ¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales?

Si, depende mucho de la categoría de la compañía y de la cantidad de datos que maneja, si bien la ley todavía no es tan especifica, creo yo que se va a especificar en el reglamento, sobre que lineamientos de seguridades especificas se debe tener, me imagino que va a depender de la categoría de datos, rubros de cada compañía; pero en términos generales si se habla mucho de los tres requisitos que son: el consentimiento, la información que se le debe dar a los titulares de datos

y la seguridad que debemos tener nosotros como compañía, para obviamente precautelar la información personal de los clientes, usuarios, trabajadores y que no haya ninguna filtración.

Pregunta Nro. 3: A su criterio ¿Cuáles son los retos que genera la implementación de la Ley Orgánica de Protección de Datos Personales dentro de los procesos internos de las empresas?

Lo principal internamente es crear conciencia sobre el uso que le damos a la información personal. Antes de la promulgación de la Ley en Ecuador no teníamos una normativa, si había disposiciones conexas en la constitución y en las demás leyes, pero no había una normativa específica para estos temas, creo que el challenge más grande es el crear conciencia dentro de todos los equipos, primero de que cierta información que recopilan es un dato personal efectivamente y segundo de la clase de seguridades que debemos de tener en el manejo de los datos. Creo que la implementación de procesos, para una compañía como la nuestra que tiene un volumen masivo de datos, si nos representa retos. El primer reto y lo más importante es el crear conciencia en los equipos de que es importante que el manejo de los datos se lo haga correctamente, creo que es el primer reto que tenemos de implementar.

Pregunta Nro. 4: ¿Cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?

El régimen sancionatorio hasta ahora me parece (creo también que va a cambiar con el reglamento) bastante proporcional. Se habla de 3 niveles de sanciones, leves, graves y muy graves, considero que se debe aclarar en el reglamento que constituye o que diferencia especialmente en lo que respecta las sanciones graves y muy graves, pero básicamente se habla mucho de que la multa va a ser proporcional al volumen del dato, al perjuicio (si es que se valora que es un perjuicio), entre otros. Hasta ahora también tenemos la posibilidad que, si la compañía esta

certificada previamente ante la autoridad como una compañía que tiene unas buenas prácticas en lo que respecta a protección de datos, se habla de que será un factor que nos ayudaría en disminuir la pena en caso de que la compañía sea sancionada.

Estoy de acuerdo con el régimen sancionatorio, pero sí creo que el reglamente tendría que ser muy específico en los temas de que constituye una violación grave, y los factores para la sanción pues esta depende del volumen de datos, depende de la intención, negligencia. Estos puntos si debiesen estar especificados.

Pregunta Nro. 5: ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

Dos años me parece un tiempo prudente, siempre y cuando tengamos reglamento y no lo tenemos. No conozco si las conversaciones que se están teniendo actualmente en la Asamblea para el reglamento se esté planteado la posibilidad de que se dé al menos un año más desde la promulgación del reglamento.

Necesitamos que el reglamento rija temas relacionado con plazos, temas relacionados con detalles más operativos para poner en prácticas los principios que indica la ley, por lo que si considero que deberíamos al menos las compañías que manejamos un volumen alto de datos (entiéndase consumos masivos, hospitales, bancos, tarjetas de créditos, etc.) si deberíamos tener un periodo de 1 año adicional desde la promulgación del reglamento para asegurarnos de que estamos completamente adecuados, ya no solo la ley sino el reglamento que regirá cuestiones mucho más operativas del día a día, pero que debemos tomar en cuenta, por ejemplo: el plazo que tenemos para contestar una solicitud de modificación de datos personales, en la ley se habla de una tiempo proporcional, en el reglamento se establecería como tiempo 15 a 30 días, 60 días; entonces

si considero que estos detalles son importantes por lo que lo correcto sería en lo que se alargue el plazo.

Entrevistado Nro. 3:

Pregunta Nro. 1: ¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?

Si, la ley fue promulgada hace apenas un año, como parte del equipo legal de la compañía dimos seguimiento al desarrollo de ley y cuando fue promulgada nos pusimos en marcha para empezar a capacitarnos, buscamos expertos para que nos ofrecieran un diagnóstico de la situación actual de la empresa en protección de datos, tuvimos acercamiento con cada área para revisar como realizan la captación de data de nuestros clientes, como los almacenaban (en soportes automatizados o en archivos físicos), entre otros. Recibimos un informe diagnóstico del tratamiento de datos que realiza la compañía, así como un informe de remediación con recomendación para reforzar ciertas prácticas en materia de protección de datos personales dentro de las empresas y con ello, dar inicio a la implementación de una cultura de protección.

Pregunta Nro. 2: ¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales?

Si y como compañía que realiza tratamiento de datos de manera masiva, estamos comprometidos al cumplimiento de las obligaciones que detalla la ley. Como parte de una compañía global, nuestras filiales en otros países nos han permitido y apoyado en los temas de protección de datos, también contratamos auditores externos para realizar un diagnóstico de los temas de seguridad que maneja la compañía, de esta manera no hemos escatimado esfuerzos en adaptarnos a cada una de obligaciones que establece la ley y aun lo continuamos haciéndolo.

Pregunta Nro. 3: A su criterio ¿Cuáles son los retos que genera la implementación de la Ley Orgánica de Protección de Datos Personales dentro de los procesos internos de las empresas?

El mayor reto que enfrentan las compañías es tener un equipo legal preparado y listo para la implementación de medidas en protección de datos, los cambios a adoptar son muchos por lo que contar con personal capacitado es una de las piezas fundamentales para lograr el éxito en la aplicación de las medidas en cada una de las áreas de la compañía. CN al ser parte de una multinacional tenemos desde global ya políticas implementadas, pues en países como México y Colombia ya ha habido un mayor desarrollo en materia de protección de datos, por lo que nos manejos ciertos criterios bajo la misma línea. Otros de los retos, y considero que el más difícil, es que las áreas sean conscientes de lo que conlleva un tratamiento de datos y como área legal poder transmitirles lo que dice la ley de manera sencilla, puesto que el tratamiento de datos conlleva términos muy técnicos, representa un gran desafío. La velocidad con la que se mueve las áreas es sumamente dinámica por lo que explicarles cómo debemos llevar ciertos procesos o que tenemos que analizar la viabilidad de alguna iniciativa que se les ocurra, es un trabajo arduo. En general eso, el poder generar conciencia de que es un dato personal y que debemos salvaguardarlos mientras se encuentren bajo nuestro tratamiento.

Pregunta Nro. 4: ¿Cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?

Se detallan multas por infracciones leves, graves y muy graves, así como se menciona medidas correctivas, tales como suspender el tratamiento de datos al responsable. Si bien las medidas se encuentran muy generales en la ley, esperamos que en el reglamento estén más específicas. Considero que las multas están alineadas con la realidad del país, pues es legislaciones

análogas como RGPD de la unión europea plantea multas más cuantiosas, pero en Ecuador se decidió un porcentaje de multa menor pues tenemos un 1%. Si bien en Ecuador no están muy detalladas o explicadas el porcentaje de la multa, estas pueden llegar a incomodar a cualquier empresario, pues representa que debe salir del bolsillo de la empresa dinero que puede ser destinado o invertido en pro de la compañía, por lo que si estas multas pueden resultar incomodas a los empresarios; en el caso de CN si llegamos a ser multados por el régimen sancionatorio no nos representaría una quiebra, pero entiendo que, para otras compañías más pequeñas, si lo seria. Como compañía lo que nos afectaría más es el tema reputacional, pues si bien entre empresas existe responsabilidad social, ambiental, entre otras, ahora también se habla se una responsabilidad de protección de datos, y esa reputación es lo que debemos conseguir para seguridad de nuestros clientes, colaboradores y futuros negocios que pactemos con otras empresas sean estas nacionales o internacionales.

Pregunta Nro. 5: ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

Es un tiempo prudente, sin embargo, considero que las empresas en el país no están viendo la magnitud de lo que implica la protección de datos de los titulares, no están tomando conciencia. En este tiempo transcurrido desde la promulgación de la normativa no se evidencia que todas las empresas se están tomando en serio la protección de datos personales, existe un tipo de relajamiento por su parte, lo que me hace pensar que una vez instaurado el régimen sancionatorio se tomaran en serio la normativa. A pesar de que aún no contemos con reglamento ni autoridad de datos, podemos replicar las acciones de otros países u otras legislaciones como el RGPD, puesto

que los motivos por los que aún no contamos con un reglamento no es culpa del legislativo, sino plenamente del Presidente de la República.

Entrevistado Nro. 4:

Pregunta Nro. 1: ¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?

Sí efectivamente la conozco, la conocí desde que estaba en proyecto en la asamblea, de hecho desde que estaba en el borrador, me gusta leer. He notado que tiene muchas fallas, muchos errores quizás técnicos, porque si tú te habrás dado cuenta hay muchos artículos en muchas este muchas partes de la ley que están incompletas o no son claras; esperemos que se solucione con el reglamento de la ley de protección de datos personales. Como te comentaba hace un rato la ley guarda muchísima relación con el reglamento europeo de Protección de Datos personales se puede decir que se derivan muchos derechos, muchas obligaciones y muchos tienen espíritu de la ley como tal de este reglamento de la Unión Europea y lo que se espera es que nosotros podamos crear al igual que otros países de Latinoamérica, de la Unión Europea y de la Comunidad Andina un régimen seguro para que pueda existir una referencia de datos segura y al mismo tiempo una libre estipulación que permita general redito para la compañía.

Pregunta Nro. 2: ¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales?

La conozco si, y es un poco más el tema de profundizar respecto a los diferentes tipos de figuras jurídicas que encuadra la ley, porque no solamente existe la figura del responsable de datos personales, también tienen al encargado de datos personales. Este trabajo es precisamente del abogado, el poder diferenciar, tú como responsable cuáles son tus derechos y obligaciones, el encargado cuáles van a ser tus derechos y obligaciones; limitar esa responsabilidad, proteger al

titular de datos personales y yo creo que muy pocos abogados se han interesado en conocer estas leyes esto es un problema porque al final de cuentas va a ser un régimen que se va a tener que aplicar de forma de compliance todas las compañías, todas las personas naturales o jurídicas que traten datos personales de los de los ciudadanos; entonces es importante que quizás haya más Academia respecto a esto para que los abogados puedan conocerlos puedan profundizar en las compañías también ahorita las compañías tienen un poco quizás el problema que tenemos en el régimen ecuatoriano que como ahora tenemos un plazo de adecuación aún no entra en vigencia el régimen sancionatorio muchas compañías se niegan o están renuentes aplicarlo en forma preventiva, pero lo que hay que hacer es justamente verlo como una medida preventiva para que al momento en que entre en vigencia, tú como como compañía que hayas aplicado todas las medidas técnicas, organizativas y legales que te permitan llegar a una responsabilidad proactiva, que es el principio general más importante de esta ley.

Pregunta Nro. 3: A su criterio ¿Cuáles son los retos que genera la implementación de la Ley Orgánica de Protección de Datos Personales dentro de los procesos internos de las empresas?

El principal reto es que las personas entiendan que esto va a ser tan importante como cualquier otro régimen que esté para las compañías. Las empresas han aplicado diferentes regímenes de protección dentro del ámbito laboral, dentro del ámbito tributario, a la final esto va a ser un régimen tan importante como esos otros regímenes legales. El primero es lograr ese entendimiento, no solamente se trata de aplicar este estas medidas, no es que se vayan a implementar una sola protección inicial tú tienes que de forma continuada y actualizada crear medidas, hacer análisis de riesgo, hacer evaluaciones de impacto en el tratamiento, y eso va a requerir una actualización constante. Entonces creo que llegar a ese entendimiento va a ser quizás

lo más importante y lo más difícil; también la capacitación del personal interno porque no solamente se trata que los grandes directivos o los representantes de la empresa adopten esto a nivel gerencial, sino que la fuerza operativa el grupo de trabajo los trabajadores en la empresa tomen conocimiento de este régimen y cuáles se van a hacer las medidas que a largo plazo van a tener que enfrentar para el cuidado de los datos personales para la Protección de Datos personales. Por ejemplo, si yo soy este parte del departamento de Recursos Humanos la información personal, incluso información sensible, de personas que este tiene que tener un cierto nivel de seguridad de confidencialidad de protección entre otros y esas personas tienen que haber socializado, tienen que tener la capacidad para poder aplicar estás tratando crear protocolos generales de la compañía sino socializar internamente esos protocolos.

Pregunta Nro. 4: ¿Cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?

Yo creo que la Ley de Protección de Datos Personales ha tratado de adaptarse en gran medida al régimen sancionatorio que aplica la unión europea, y el problema aquí es el desconocimiento a esta materia, que quizás en otros países, ya tenía desde hace muchísimo tiempo atrás un nivel diferente de educación, conocimiento, a nivel empresarial, a nivel académico, entonces la aplicación de estas medidas y las medidas de sí mismo, yo creo que van a causar a lo largo de este tiempo que va a tardar para la aplicación, y entrada en vigencia en mayo del 2023, va a causar mucha controversia porque son sanciones muy altas, estamos hablando desde el 0.1 al 0.7 para las infracciones leves y el 0.7 al 1% para infracciones graves, entonces van a ser sanciones sumamente cuantiosas y las medidas correctivas, si es que tú haces un análisis de la ley, la ley te dice tu vas a tener aplicar medidas técnicas, organizativas, legales dentro de esto tú vas a poder sacar certificaciones, tú vas a poder hacer análisis de riesgo, tú vas a poder ser evaluación impacto,

no te da un listado categórico o taxativo de cuáles van a ser esas medidas, y es correcto porque estas medidas van a ser independiente de acuerdo a la necesidad de cada negocio y de cada sector empresarial; entonces por eso es que no se podía hacer un listado taxativo y deberían de existir más bien principios respecto a esto. Pero en esta aplicación y en este régimen, como las empresas y los abogados que quizás no son expertos en la materia no van a conocer precisamente qué es lo que mejor se va a adecuar para la compañía; entonces por eso yo hago mucho énfasis en el tema de la academia es importante, que haya más tesis como las que tú estás haciendo al respecto a profundizar que es un dato personal, cuáles son los tipos de medidas: porque hablamos de técnicas y organizativas, pero ¿cuáles son esas medidas? ¿qué medidas pueden existir de acuerdo al nivel de negocio?, tiene evidentemente no va a ser lo mismo una protección de la información que tenga cervecería a la protección de la información que tenga la tienda de nuestro barrio, son medidas diferentes son acciones diferentes respecto al responsable y el encargado del tratamiento de datos personales, por lo que yo creo que eso es lo importante que hay que destacar.

Pregunta Nro. 5: ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

Desde el deber ser te puedo decir que sí, pero en el ser no. El problema es porque recién las empresas lo están implementando, de manera general desde a mediados de este año de lo que yo he tenido conocimiento evidentemente. Recién a mediados de año a pesar de que la ley entró en vigor desde el año 2021 recién ahora se están preocupando por hacerlo. Pero esto es un nicho muy muy pequeño que no se equipara al nivel empresarial ecuatoriano, que en porcentajes creería que la mayoría empresa no tienen conocimiento todavía de este régimen y que aunque lo tuvieran no quieren aplicarlo, porque este es un problema tanto de las personas naturales o jurídicas en

Ecuador que no tienen una cultura de prevención, porque la ley de forma preventiva te está diciendo que va a aplicar esas medidas correctivas, para que tú en el plazo de 2 años puedan implementarlas, pero como no hay mucha cultura de prevención estas compañías siempre lo que te tiende es que ya entre en vigencias y que se empiece a sancionar para recién empezar a aplicar las medidas, este considero que es el mayor problema de las empresas ecuatorianas y lo que hace que este tiempo de dos años sea muy poco.

6.3 Análisis estadístico

Una vez aplicadas las técnicas de encuesta y entrevista, se puede concluir lo siguiente:

De las encuestas realizadas a los profesionales del Derecho, se puede evidenciar que conocen la Ley Orgánica de Protección de Datos Personales, están al tanto de la entrada en vigencia de la misma, pues dada la actualidad en la que vivimos, la tecnología se a acentuado como protagonista en diversos aspectos de la vida en la sociedad, y el Derecho no es la excepción, de ahí nace la importancia de la nueva LOPDP y la necesidad de que los abogados litigantes la conozcan. Afirman conocer las obligaciones que deben cumplir las empresas para evitar incurrir en infracciones, así como las medidas de seguridad que deben implementar para proteger los datos de los titulares. Siguiendo esta línea de pensamiento, con certeza manifiestan haberse informado del régimen sancionatorio que entrará en vigencia el 26 de mayo del 2023, y destacan su parecido con el reglamento europeo. Con todo lo anteriormente mencionado, se puede evidenciar en las estadísticas, que los profesionales encuestados manifiestan conformidad con el hecho de establecer una prórroga para la entrada en vigencia del régimen sancionatorio, puesto que, el acoplarse a lo que establece la Ley requerirá grandes esfuerzos a nivel económico, tecnológico y de personal, mismos que no todas las empresas están en condiciones de hacerlo en un corto periodo de tiempo.

Las respuestas otorgadas por las personas entrevistadas nos permiten comprender dos puntos de vistas de la realidad de las empresas del sector privado ecuatoriano en lo que respecta a la aplicación de la Ley Orgánica de Protección de Datos Personas. El primer punto de vista es el de los abogados que trabajan dentro de las organizaciones y que actualmente se encuentran en la labor de implementar los procedimientos, medidas y herramientas en lo técnico, físico, administrativo, jurídico y organizativo para ejecutar los requerimientos y obligaciones dispuestas en la ley para las empresas en calidad de responsables, y por otra parte el punto de vista de dos abogados pertenecientes a grandes firmas jurídicas que asesoran y guían a las organizaciones al cumplimiento de la LOPDP.

En las opiniones de cada uno de los profesionales entrevistados se puede puntualizar que conocen la ley desde que fue promulgada, y que están informados de las obligaciones estipuladas para los responsables de datos personales, para el caso concreto de la presente investigación las empresas del sector privado del país, demostrando que conocen la realidad jurídica de la situación planteada. Concuerdan que la LOPDP genera grandes retos para las organizaciones que traten datos personales; uno de los retos mencionados por la mayoría de los entrevistados es la falta de capacitación de que existe y lo poco que se conoce lo que abarca la protección de datos, es decir no se le da la importancia que representa; además ello todos coinciden y mencionan reiteradamente la falta del desarrollo normativo en la materia, pues si bien ha transcurrido más de un año de la promulgación de la ley aun el país con un reglamento que profundice en ciertas cuestiones que son plenamente de interés para los responsables; bajo este orden tampoco se ha creado la autoridad de protección de datos que si bien es un ente regulador, también tiene entre sus facultades el emitir directrices y lineamientos que servirían de guía para las empresas. Con respecto al régimen sancionatorio y medidas correctivas, la opinión obtenida de los entrevistados delata que las multas

no son del todo claras por lo que se espera que en el reglamento se explique de manera detallada la distinción entre presunto cometimiento de infracciones graves o muy graves para la imposición de medidas correctivas, así como los parámetros para la imposición de sanciones. Finalmente, sobre la pregunta relacionada a la disposición transitoria de ley que establece el tiempo de dos años desde su promulgación para que empiece a operar el régimen sancionatorio y las medidas correctivas, los profesionales entrevistados concuerdan que tiempo de dos años sería prudente solo en el caso de que el sistema de protección de datos personales se encuentre completo, pero no es el caso; por lo que los dos años establecidos es insuficiente al no contar con el reglamento de ley, debido a que retrasa la adecuación de las empresas. Sin embargo, acotan que prolongar demasiado el tiempo para la aplicación de multas puede generar que las empresas se relajen y no tomen seriedad a la aplicación de la normativa.

La intención del legislador es buena, pero hay puntos que deben ser tratados y discutidos con gran seriedad, para que la ley pueda tener el impacto deseado, y sobre todo cumplir a cabalidad su objetivo: proteger los datos de los titulares.

7. Discusión

7.1 Verificación de Objetivos

Es pertinente para realizar la verificación de objetivos, remitirnos a los establecidos en el anteproyecto del presente trabajo de titulación.

7.1.1 Objetivo General.

"Determinar los mecanismos objetivos para el tratamiento de datos personales con el fin de proteger, preservar y viabilizar la protección de datos personales y que retos enfrentan las compañías que realizan tratamiento de datos personales al implementar las disposiciones previstas en la Ley Orgánica de Protección de Datos Personales"

El presente objetivo ha sido verificado mediante el apartado de marco teórico, en donde de forma clara se ha estudiado el derecho a la protección de datos personales, analizando su reseña histórica, desde el surgimiento en el Derecho Anglosajón con el concepto de "*Privacy*", en donde se dio a conocer que antes de la protección de datos personales se desarrolló el concepto de intimidad personal, considerado como el derecho a estar solo "to *be alone*", así mismo se estudió en como Inglaterra, después de los estadounidenses, desarrolló este concepto, con una incansable lucha que comenzó con el proyecto de Mancroft, hasta lo que se conoce actualmente como la "Data Protection Act".

Se evidenció que el derecho a la protección de datos personales, surge como un complemento al derecho a la intimidad, pero con el avance tecnológico estos conceptos presentan una contradicción, que de tratarlos conjuntamente como si fuesen uno solo, los desnaturalizaría. Es por eso, que surgió la necesidad de individualizarlos, siempre en pro de la protección de datos de los titulares, gozando así de una firme tutela jurídica.

Se analizó la legislación ecuatoriana (Constitución de la República del Ecuador y Ley Orgánica de Protección de Datos Personales) en todo lo que se refiere a la protección de datos personales, y se contrastó con la legislación comparada. Por todo lo anteriormente dicho, el objetivo general ha quedado plenamente verificado.

7.1.2 Objetivos Específicos.

Primer Objetivo: "Establecer las medidas que deben implementar los responsables de datos personales, para adecuarse a la Ley Orgánica de Protección de Datos Personales"

El presente objetivo ha sido verificado mediante el desarrollo del marco teórico, que en su apartado pertinente se ha estudiado y analizado los diversos tipos de medidas de seguridad que deben implementar las personas encargadas del tratamiento de datos personales, siendo estas: medidas organizativas, medidas técnicas, medidas jurídicas, medidas administrativas. Si bien es cierto la LOPDP no especifica las medidas a aplicarse con el desarrollo del marco teórico en el presente trabajo de investigación, se ha podido dar a conocer de forma clara los esfuerzos que deben realizar las empresas para la protección de datos personales de sus titulares.

La norma específica que las medidas de seguridad deben aplicarse de acuerdo a las actividades que desarrollan las empresas y su giro de negocio, de las técnicas de encuesta, en la segunda pregunta (¿Conoce usted acerca de las medidas de seguridad que deben implementar las empresas, así como las obligaciones que deben en su calidad de responsables, para garantizar la protección de datos personales?) y entrevista en la segunda pregunta (¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables para garantizar la protección de datos personales?) realizadas a profesionales del derecho y especialistas en la materia se ha logrado evidenciar que si bien es cierto la norma menciona algunos tipos de medidas de seguridad, no existe una clara definición de las mismas, así como no se tiene claro en qué circunstancias cada

empresa deberá aplicarlas, por lo tanto consideran que lo que está establecido en la LOPDP es insuficiente..

Con lo anteriormente detallado el primer objetivo específico ha quedado plenamente verificado.

Segundo Objetivo: "Conocer las consecuencias sancionatorias para las empresas si no se adecuan a la normativa"

El presente objetivo ha sido verificado en el marco teórico que en su apartado pertinente ha permitido evidenciar cuales son las consecuencias que establece el régimen sancionatorio en la LOPDP. Especifica no solo sanciones de carácter administrativo, sino también las de carácter económico. Podemos darnos cuenta entonces, que, nuestra legislación sigue el modelo europeo del reglamento general de protección de datos personales, adaptando las multas al volumen de negocio. Además de las encuestas, en la tercera pregunta (La LOPDP establece un régimen sancionatorio para aquellas empresas que no se acoplen a lo establecido en el texto legal ¿tiene usted conocimiento acerca de dicho régimen?) y entrevistas en su acuarta pregunta (¿cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?) realizadas podemos percatarnos de que los profesionales del derecho en su gran mayoría conocen lo relacionado a las sanciones que se aplicarán una vez que entre en vigencia las medidas correctivas el mes de mayo, por cometimiento de infracciones ya sean leves, graves o muy graves.

Con lo anteriormente manifestado se ha verificado el segundo objetivo específico.

Tercer Objetivo: "Sugerir una prórroga a la aplicación de las medidas correctivas y el régimen sancionatorio"

El presente objetivo específico, tema central de mi investigación ha sido verificado mediante la técnica de encuestas, en las cuales en su última pregunta (¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?), la totalidad de los profesionales del derecho encuestados de forma unánime manifestaron su inconformidad con el tiempo establecido en la norma para la entrada en vigencia del régimen sancionatorio.

Además de las entrevistas realizadas a especialistas en la materia, a quienes se les realizo la misma pregunta podemos evidenciar su inconformidad con lo manifestado en la norma, argumentando que nuestro país no está listo aun para cambios de tal magnitud, considerando entonces que dos años son insuficientes. Los esfuerzos que deben realizar las empresas para acoplarse a la norma son gigantescos, implican grandes cambios no solo a nivel de la organización, sino también a nivel tecnológico, lo que produciría grandes gastos que en ocasiones no están listos para asumir o no tienen los presupuestos necesarios. Concuerdo con lo manifestado por los entrevistados debido a que no es suficiente con la expedición de la ley como tal, es necesario un reglamento en el cual se establezcan las directrices a seguir para el cumplimiento correcto de la norma, esto sin dejar de lado la inexistente autoridad de protección de datos personales y la superintendencia que se supone ya debió haber sido creada, estamos a un mes de la entrada en vigencia de las medidas correctivas y el régimen sancionatorio en general, pese a ello las empresas no se encuentran en las condiciones para adaptarse a lo exigido por la norma. Tomemos como ejemplo a Europa, que pese a que cuenta con países mucho más desarrollados a nivel organizativo y tecnológico no pudo adaptarse en su totalidad al reglamento general de protección de datos personales expedidos por la unión europea. Queda claro entonces que el tiempo de dos años es insuficiente por lo cual es pertinente ampliarlo mediante una reforma.

Con lo anteriormente manifestado el tercer objetivo específico ha quedado en su totalidad verificado.

7.4 Fundamentación Jurídica de la Propuesta de Reforma.

Los problemas que en la actualidad existen es gracias al poco interés o conocimiento que las personas tienen sobre sus datos personales, donde se verían perjudicados o vulnerados por terceras personas, llevando consigo un problema para uno de los derechos fundamentales que es nuestra intimidad, honor, buen nombre. Con ello podemos indicar en el Artículo 92 de la Constitución de la República del Ecuador indica el acceso de los datos personales, pero el interés es buscar soluciones, donde los datos se protejan desde el momento de su recogida hasta que llegue a su destino, de la misma manera indicar la importancia de los mismo ya que las personas en la actualidad solo conocemos el cómo dar información mas no como se protege nuestra información personal.

Como se ha evidenciado a lo largo de la investigación, la regulación de la protección de datos personales es completamente nueva en el país. La reciente LOPDP establece dentro de su normativa los derechos de los titulares, así como el marco para un tratamiento de datos personales legítimo y adecuado por parte de los responsables de datos; las obligaciones a las que están sujetos los responsables sean estos personas naturales o jurídicas; y el régimen sancionatorio para los casos de incumplimiento del mandato de ley.

Todo este sistema de protección de datos que debe ser conocido por los titulares y aplicado por las empresas del país. En este contexto el dar cumplimientos a las obligaciones que estipula la ley, representa grandes retos para las empresas que, por su giro de negocio traten datos personales, pues deben ejecutar cambios dentro de la organización, como aplicar medidas de seguridad administrativas, jurídicas, físicas, técnicas y organizativas, las cuales deben ser verificadas,

evaluadas y valoradas periódicamente; las empresas también deben llevar a cabo políticas de protección, así como utilizar métodos de análisis y gestión de riegos, entre otras obligaciones mencionadas en la ley.

Todas las implementaciones mencionadas deben ser adaptadas en cada área de la compañía y además de ello generar conciencia de lo que representa tratar un dato personal, pues este representa uno de los mayores retos dentro de las organizaciones. Por ello el trabajo que deben realizar las empresas para ejecutar y cumplir con las obligaciones detalladas en la ley es arduo, sin embargo, la ley a pesar de tener estipuladas estas obligaciones, solo las enumera mas no las detalla ni profundiza en lo que implica cada imposición.

Si bien la normativa sanciona el incumpliendo de las obligaciones previstas, su efecto fue suspendido por dos años desde la promulgación de la ley, para darle la oportunidad a las empresas de adecuarse, sin embargo ha transcurrido más de un año desde la mencionada promulgación, y aun no contamos con un reglamento que profundice los preceptos para la ejecución de la ley, al igual que no se ha creado la Autoridad, ente que además de salvaguardar la protección de los datos de los titulares, serviría de guía para las empresas, pues dentro de sus atribuciones y facultades se establece atender consultas, establecer directrices para la selección de medidas de seguridad, emitir guías de la normativa, entre otras facultades que claramente pueden guiar a las compañías a efectuar un tratamiento legítimo de datos personales. En este sentido, a menos de un año para que empiece a operar el régimen sancionatorio, el sistema de protección no se encuentra completo, lo que genera que las empresas no cuenten con todos los instrumentos jurídicos para poder cumplir con las obligaciones. Como se mencionó con anterioridad, la temática de datos personales es nueva en el país, son pocos los expertos en el tema, y acceder a asesorías puede incidir es gastos adicionales para las pequeñas empresas del país, al igual que no tener guías ni contar con ayuda

de expertos podría generar que estas empresas incurran en incumplimiento a la ley y sean sancionadas, con multas que podrían resultar en afectaciones económicas y en el peor de los casos en quiebra para la organización.

8. Conclusiones

Realizado el estudio del presente objeto de investigación, y verificados los objetivos tanto general como específicos e hipótesis, los resultados obtenidos por la presente tesis se ha podido arrojar las siguientes conclusiones:

1. La protección de datos personales surge como un complemento al derecho a la intimidad, definido por los anglosajones como el derecho a estar solo "to be alone" a no ser perturbado, a que el individuo pueda desarrollar su personalidad sin injerencias externas, pero con la evolución de los conceptos, se llegó a la conclusión de que es un derecho totalmente independiente.
2. La protección de datos personales, antes del 2021 no se encontraba regulada por ninguna Ley especial, sin embargo, nuestra constitución ya la reconocía como un derecho, con la llegada de la LOPDP se pudo evidenciar un gran avance en la materia.
3. La llegada de la Ley Orgánica de Protección de Datos Personales ha tenido un impacto considerable en la sociedad ecuatoriana, sobre todo en el sector corporativo, pues la ley trae consigo una seria de obligaciones con las que tienen que cumplir las empresas, para garantizar la protección de los datos personales de sus clientes, colaboradores y proveedores, dado que si se incumple con las disposiciones de ley pueden ser objeto de sanciones.
4. Las obligaciones para las compañías en calidad de responsables de datos personales son de variado alcance, pues deben definir las actividades de su tratamiento, realizar evaluaciones impacto de las operaciones del tratamiento y gestiones de riesgos, implementar medidas de seguridad físicas, jurídicas, técnicas organizativas y administrativas, llevar a cabo planes de capacitación para todos los colaboradores de la

empresa, entre otras obligaciones mencionadas en la ley y a las necesidades de cada empresa.

5. Es imperativa la necesidad de elaborar un proyecto de reforma a la disposición transitoria de la LOPDP, puesto que el implementar, mantener, revisar y mejorar continuamente sistemas y medidas de seguridad para el tratamiento de esos datos, sumados a otros factores como la falta de normativa como el reglamento de ley y guías para las compañías que no puedan costear asesorías especializadas, genera una problemática para las empresas que buscan adaptarse a le ley, por lo que el tiempo de dos años otorgados no es suficiente, pues de iniciarse el régimen sancionatorio sin estar listos puede traer grandes afectaciones económicas e incluso a la quiebra de las compañías.

9. Recomendaciones

1. Exhortar a los profesionales del derecho a una preparación adecuada en materia de Protección de datos Personales, puesto que, si bien es cierto aun es un tema novedoso, la sociedad informática en la que nos encontramos justifica la tutela de los datos de los titulares y en esa misma línea exige un adecuado conocimiento de los abogados defensores.
2. Incitar a la Asamblea Nacional del Ecuador se expida el Reglamento a la Ley Orgánica de Protección de Datos Personales con la finalidad de reglamentar los preceptos y disposiciones establecidos en la mencionada ley, y que otorgue desarrollo a las obligaciones con las que debe cumplir los responsables, en las directrices para designar al delegado de datos personales, se profundice en el tema de las sanciones, entre otros.
3. Exhortar al Consejo de Participación Ciudadana y Control Social agilizar la creación de la "Autoridad de Protección de Datos Personales" a través de una Superintendencia, con el propósito de que se atienda al interés general, y que los responsables de datos personales puedan acceder a las directrices y lineamientos que deberá emitir la autoridad, al igual de poder acceder a realizar sus consultas en materia de protección de datos personales, entre otras facultades.
4. A la Asamblea Nacional que, se prorrogue el tiempo de dos años establecido en las disposiciones transitorias de la LOPDP para la aplicación de las medidas correctivas y el régimen sancionatorio en el país, en al menos tres años contados desde la entrada en vigencia de la ley o en su defecto de la entrada en vigencia del Reglamento a la "Ley Orgánica de Protección de Datos Personales".

9.1 Proyecto de reforma legal

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

EL PLENO

CONSIDERANDO

Que, la Constitución de la República del Ecuador 2008 en su artículo 1 establece que el Ecuador es un estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada previstas en la Constitución.

Que, el artículo 66 numerales 19 de la Norma Suprema reconoce y garantiza a las personas: "El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley";

Que, Que, "la protección de datos personales forma parte de los ejes estratégicos para la construcción de la sociedad de la información y el conocimiento en el Ecuador conforme el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018";

Que, la Protección de Datos Personales, para el sector corporativo tiene gran importancia para la economía del país, pues representa la digitalización de los negocios empresariales y que Ecuador se convierta en un foco de inversión extranjera.

Que, es necesario reformar las disposiciones transitorias de la LOPDP, que contemple una prórroga a las medidas correctivas y al régimen sancionatorio, para garantizar empresas privadas capacitadas.

Que, en la actualidad las disposiciones no establecen un tiempo determinado para la expedición del reglamento a la Ley.

Que, es necesario realizar una socialización de proyecto de ley con las y los ecuatorianos para evitar vulneraciones a su vida privada e íntima. Con respecto a la protección de los datos personales. Dando como resultado una Ley Orgánica para la Protección de Datos Personales En el Ecuador.

En ejercicio de las atribuciones conferidas por el artículo 120, numeral 6, de la Constitución de la República del Ecuador, y el artículo 9, numeral 6, de la Ley Orgánica de la Función Legislativa, expide la presente:

“PROYECTO DE LEY REFORMATORIO A LAS DISPOSICIONES TRANSITORIAS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES”

PRIMERA: Sustitúyase la disposición transitoria primera de la Ley Orgánica de Protección de Datos Personales, por el siguiente texto:

PRIMERA. “Las disposiciones relacionadas con las medidas correctivas y el régimen sancionatorio entrarán en vigencia en tres años contados a partir de la publicación de esta Ley en el Registro Oficial, en el transcurso de este tiempo los responsables y encargados del tratamiento de datos personales se adecuarán a los preceptos establecidos dentro de esas disposiciones, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales. El resto de las disposiciones establecidas en esta Ley entrarán en vigencia conforme se establece en la Disposición Final de esta Ley”.

SEGUNDA: Incorpórese como disposiciones transitorias quinta y sexta de la Ley Orgánica de Protección de Datos Personales, los siguientes textos:

QUINTA. “El presidente de la República expedirá en ciento ochenta días el Reglamento de la presente Ley”.

SEXTA. “En el plazo máximo de ciento ochenta días a partir de la publicación de la presente Ley en el Registro Oficial, se conformará La Superintendencia de Protección de Datos Personales. La o el Superintendente será nombrado dentro del plazo de ciento veinte días adicionales”.

DISPOSICIÓN FINAL

La Ley Orgánica de Protección de Datos Personales en el Ecuador entrará en vigencia a partir de la fecha de su publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los doce días del mes de abril de dos mil veintitrés.

…….

DR. VIRGILIO SAQUICELA ESPINOZA

Presidente

…….

ABG. ÁLVARO SALAZAR PAREDES

Secretario General

10. Bibliografía

Acurio del Pino, S. (s.f.). *Delitos Informáticos: Generalidades.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Agencia Española de Protección de Datos. (2019). *Agencia Española de Protección de Datos*. Obtenido de https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-

Alexy, R. (1993). *Teoría de los Derechos Fundamentales.* Madrid: Centro de Estudios Constitucionales.

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

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito: Registro Oficial Suplemento 459 de 26-may.-2021.

Banizar, B. (2011). The Right to Information and Privacy: Balancing Rights and Managing Conflicts. Obtenido de http://wbi.worldbank.org/wbi/Data/wbi/wbicms/files/drupal-acquia/wbi/Right%20 to%20Information%20and%20Privacy.pdf.

Berlin, I. (1967). *Two concepts of Liberty* (Political philosophy ed.). Oxford: Oxford University.

Bodero & Asociados. (2022). *M.Bodero & Asociados*. Obtenido de https://boderoyasociados.com/seguridad-de-la-informacion-proteccion-de-datos-personales/

Bustamante, J. (2007). Los nuevos derechos humanos: gobierno electronico e informatica comunitaria. *Revista venezolana de informacion, tecnología y conocimiento, 4*(2), 13-27.

Carisio, E. (2018). *mdcloud*. Obtenido de #ADN CLOUD Innovación en la Sociedad Digital: https://blog.mdcloud.es/que-es-big-data-y-para-que-sirve/#Que_es_Big_Data_y_para_que_sirve

Casal Tavasci, J. (s.f.). *Protección Data.* Obtenido de https://protecciondata.es/interes-vital/

Clímaco , E. (2012). *Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento.* Tesina, Universidad Carlos III de Madrid, Getafe. Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM_MEADH_Ernesto_Climaco.pdf?sequence=1&isAllowed=y

Congreso Constituyente de México. (5 de febrero de 1917). Consitución Política de los Estados Unidos Mexicanos. España. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Cortes Generales. (29 de octubre de 1992). Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.* España. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Cova Fernandez, E. (2010). Derechos humanos y derechos digitales en la sociedad de la información. *Universidad nacional de eduación a distancia*, 64-70.

CPCCS. (s.f.). *Consejo de Participación Ciudadana y Control Social*. Obtenido de https://www.cpccs.gob.ec/designacion-de-autoridades-nuevo-cpccs/

Davara Rodriguez, M. (2006). *Manual de Derecho Informático.* Madrid: Thompson Aranzadi.

Eguiguren Praeli, F. (s.f.). *La Libertad de Expresión e Información y el Derecho a la Intimidad Personal.* Lima: Palestra Editores.

García Falconí, J. (s.f.). *El juicio especial por acción de habeas data* (Primera ed.). Quito.

General Data Protection Regulation. (2016). *intersoft consulting*. Obtenido de https://gdpr-info.eu/

IDAIP. (s.f.). Guia Medidas de Seguridad para la Protección de Datos Personales. *Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales*, 9-17. Obtenido de https://www.idaip.org.mx/archivos/formatos/Promocion_Vinculacion/Gu%C3%ADa%20medidas%20de%20seguridad.pdf

informática. (s.f.). *Informática*. Obtenido de https://www.informatica.com/services-and-training/glossary-of-terms/data-transfer-definition.html

Instituto Nacional de Ciberseguridad. (s.f.). PROTECCIÓN DE LA INFORMACIÓN. *incibe*, 6-7. Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Las Cortes . (27 de septiembre de 2011). Constitución Española. *Constitución española*. España: Senado de España.

Ley del Censo, Derecho a la Personalidad y Dinidad Humana, ref. 1 BvR 209/83 (Tribunal Constitucional Alemán 15 de diciembre de 1983). Obtenido de https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485

Losano G, M. (1989). *Los orígenes del "Data Protection Act" inglesa de 1984.* Madrid: Centro de Estudios Constitucionales.

Lutkevich, B. (s.f.). *Tech Target* . Obtenido de Data Management: https://www.techtarget.com/searchdatamanagement/definition/database

MacIntyre Cooley, T. (1895). *Elements of Torts.* Chicago: Callaghan and Company. Obtenido de https://archive.org/details/cu31924019221732/page/n4/mode/1up?view=theater

Moisés Barrio, A. (2018). *CiberDerecho, bases estructurales, modelos de regulación e instituciones de gobernanza de internet.* Valencia, España: Tirant Lo Banch.

Naranjo, L. (19 de febrero de 2018). El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en el Ecuador. *Revista de Derecho, 1*(27).

Ordoñez Pineda, L., Correa Quezada, & Correa, A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado y Comunes, 2*. Obtenido de https://www.redalyc.org/journal/6842/684272393004/html/

Parlamento Europeo. (27 de abril de 2016). Reglamento General de Protección de Datos. *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016*. Diario Oficial de la Union Europea. Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Peces Barba, G. (1988). *Sobre el puesto de la historia en el concepto de los derechos fundamentales.* Madrid: Eudema.

PRIMICIAS. (2023). Multas por la Ley de Protección de Datos comenzarán en mayo. Obtenido de https://www.primicias.ec/noticias/economia/ley-proteccion-datos-personales-sanciones/

proofpoint. (2023). *proofpoint*. Obtenido de https://www.proofpoint.com/es/threat-reference/personal-identifiable-information

Queen’s most Excellent Majesty, Lords Spiritual and Temporal, Commons, & Parliament. (23 de mayo de 2018). Data Protection Act 2018. *Data Protection Act 2018*. United Kingdom. Obtenido de https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Quiroga Lavié, H. (1995). *Derecho a la intimidad y objeción de la conciencia.* Bogotá: Universidad externado de Colombia.

RAE. (s.f.). *Real Academia Española*. Obtenido de https://dle.rae.es/intimidad

Razza, C. (2021). *La transferencia internacional de datos personales en Ecuador.* Ecuador: UDLA Ediciones.

Rodríguez Mourullo , G. (2019). *Manual de Introducción al Derecho Penal.* MADRID: Agencia Estatal Boletín Oficial del Estado. Obtenido de https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DP-2019-110

Rodríguez, J. F. (2019). *Figuras y responsabilidades en el tratamiento de datos personales.*

Santos García, D. (2012). *Nociones generales de la Ley Orgánica de Protección de Datos y su reglamento: adaptado alRD 1720/2007 de 21 de diciembre.* Madrid: Tecnos.

Sentencia N.° 025-15-SEP-CC, N.° 0725-12-EP.a (Corte Constitucional del Ecuador 4 de febrero de 2015). Obtenido de http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/2f1e577c-bc9e-481b-9588-d34db2cac439/0725-12-ep-sen.pdf?guest=true

Smedinghoff, T. (2019). *An Overview of Data Security Legal Requirements for All Business Sectors.* Chicago. Obtenido de https://www.researchgate.net/profile/Thomas-Smedinghoff

Stuart Mill, J. (1959). *On Liberty. Prefaces to Liberty*. Boston: Beacon press.

Tech Target. (2017). *Tech Target*. Obtenido de Tech Target: whatls.com

Troncoso Reigada, A. (2010). *La protección de datos personales: en busca del equilibrio.* Valencia: Tirant lo Blanch.

UNIR. (s.f.). *UNIR La Universidad en Internet*. Obtenido de UNIR La Universidad en Internet: https://www.unir.net/derecho/revista/reglamento-general-de-proteccion-de-datos/

Villalba Fiallos, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *FORO Revista de Derecho*(27), 8.

Villanueva Haro, B. (2007). La funcionalidad y delimitación de las medidas correctivas como mecanismo regulador de las conductas económicas negativas en el mercado y el respeto al principio non bis in idem. *Revista Internauta de Práctica Jurídica*(19), 12-28. Obtenido de https://www.uv.es/ajv/art_jcos/art_jcos/num19/RIPJ_19/EX/19-17.pdf

11. Anexos

Anexo 1. Oficio de Aprobación

Universidad Nacional de Loja | Facultad Jurídica Social y Administrativa | Carrera de Derecho

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA CARRERA DE DERECHO

CERTIFICACIÓN

Loja, 26 de abril de 2023

Dr. Jeferson Vicente Armijos Gallardo, Mg. Sc.

DOCENTE DE LA CARRERA DE DERECHO DE LA FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA DE LA UNIVERSIDAD NACIONAL DE LOJA,

CERTIFICO

Que el presente trabajo de titulación, elaborado por la Señorita **Lady Carolina Pardo Guamán,** titulado "**El Tratamiento de Datos Personales y su Regulación Normativa en el Ecuador Según las Nuevas Tecnologías de la Información y la Comunicación"** ha sido dirigido de acuerdo a los requisitos previstos para el trabajo de investigación, así mismo se ha corregido y revisado en su forma y contenido de conformidad a las normas de graduación vigentes en el Art. 229 del Reglamento de Régimen Académico de la Universidad Nacional de Loja 2021; por lo que, en cumplimiento al Art. 231 del citado reglamento procedo a emitir satisfactoriamente el certificado de cumplimiento del trabajo de titulación aprobado, certificando que la ejecución del presente trabajo se encuentra ejecutado en un 100%, por lo que autorizo al autor que continúe con el trámite administrativo de aptitud legal para su presentación, sustentación y defensa ante el Honorable Tribunal de Grado, de conformidad a los artículos 235, 236 y 237 del Reglamento antes mencionado.

Atentamente.-

JEFERSON VICENTE ARMIJOS GALLARDO
Firmado digitalmente por JEFERSON VICENTE ARMIJOS GALLARDO
Fecha: 2023.04.26 15:36:52 -05'00'

Jeferson Vicente Armijos Gallardo Mg. Sc
DIRECTOR DEL TRABAJO DE TITULACIÓN

Anexo 2. Certificación de Traducción al Abstract

Loja, 20 de Julio del 2023

Lic. Jhessica Alexandra Jumbo Obaco

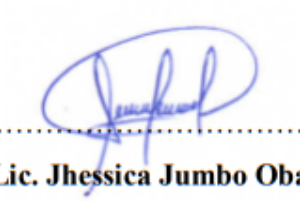
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN MENCIÓN INGLES

CERTIFICO:

Yo, Lic. Jhessica Alexandra Jumbo Obaco con C.I. 110512565-0; certifico que he traducido el Abstract del Trabajo de Integración Curricular o de Titulación con el nombre **"EL TRATAMIENTO DE DATOS PERSONALES Y SU REGULACIÓN NORMATIVA EN EL ECUADOR SEGÚN LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN"**

Se otorga el siguiente certificado al interesado para los fines legales pertinentes.

Atentamente. –



.....

Lic. Jhessica Jumbo Obaco

C.I. 110512565-0

LICENCIADO EN CIENCIAS DE LA EDUCACIÓN MENCIÓN INGLES

Anexo 3. Certificación de Tribunal de Grado

CERTIFICACIÓN DEL HONORABLE TRIBUNAL DE GRADO

Loja, 17 de julio de 2023

En nuestra calidad de Tribunal Calificador del Trabajo de Titulación denominado: **El tratamiento de Datos Personales y su Regulación Normativa en el Ecuador según las Nuevas Tecnologías de la Información y la Comunicación**, de la autoría de la señorita egresada Lady Carolina Pardo Guamán, portadora de la cédula de ciudadanía Nro. 1150097630, previo a la obtención grado de Licenciada en Jurisprudencia y título de Abogada, certificamos que se ha incorporado las observaciones realizadas por los integrantes del Honorable Tribunal de Grado, por tal motivo se procede a la calificación y aprobación del trabajo de integración curricular, en consecuencia se autoriza la continuación de los trámites pertinentes para su publicación, sustentación y defensa pública.

APROBADO

Dr. Guilber René Hurtado Herrera, Mg. Sc.
PRESIDENTE

Dr. Fernando Filemón Soto Soto, Mg. Sc.
VOCAL PRINCIPAL

Dr. Servio Patricio González Chamba, Mg. Sc.
VOCAL PRINCIPAL.

Anexo 4. Formato de Encuestas a profesionales del Derecho

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENCUESTA

Estimado abogado (a): 30 variables

Me encuentro desarrollando mi investigación jurídica en la modalidad de tesis titulado: **"EL TRATAMIENTO DE DATOS PERSONALES Y SU REGULACIÓN NORMATIVA EN EL ECUADOR SEGÚN LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNIDAD"** Por lo tanto, requiero de su criterio jurídico respecto a mi investigación. Le ruego se sirva contestar las siguientes interrogantes:

PREGUNTAS

1. **¿Conoce usted acerca de la nueva Ley Orgánica de Protección de Datos Personales?**

SI ( ) NO ( )

¿Por qué?

---

2. **¿Conoce usted acerca de las medidas de seguridad que deben implementar las empresas, así como las obligaciones que deben en su calidad de responsables, para garantizar la protección de datos personales?**

   SI ( ) NO ( )

   ¿Por qué?

   ---

3. **La LOPDP establece un régimen sancionatorio para aquellas empresas que no se acoplen a lo establecido en el texto legal ¿tiene usted conocimiento acerca de dicho régimen?**

   SI ( ) NO ( )

   ¿Por qué?

   ---

4. **A su criterio ¿Considera que las empresas se verían afectadas una vez entrasen en vigencia las medidas correctivas debido a la falta de un reglamento a la LOPDP, así como la inexistencia de la Autoridad pertinente?**

   SI ( ) NO ( )

   ¿Por qué?

   ---

5. **¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?**

SI ( ) NO ( )

¿Por qué?

GRACIAS POR SU COLABORACIÓN

Anexo 5. Formato de Entrevistas a especialistas en la materia

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA

Estimado entrevistado (a):

Me encuentro desarrollando mi investigación jurídica en la modalidad de tesis titulado: **"EL TRATAMIENTO DE DATOS PERSONALES Y SU REGULACIÓN NORMATIVA EN EL ECUADOR SEGÚN LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNIDAD"** Por lo tanto, requiero de su criterio jurídico respecto a mi investigación. Le ruego se sirva contestar las siguientes interrogantes:

1. ¿Conoce usted acerca de la Ley Orgánica de Protección de Datos Personales?

   _____

   _____

   _____

2. ¿Conoce las obligaciones que deben cumplir las empresas, en su calidad de responsables, para garantizar la protección de datos personales?

_____

_____

_____

3. A su criterio ¿Cuáles son los retos que genera la implementación de la Ley Orgánica de Protección de Datos Personales dentro de los procesos internos de las empresas?

_____

_____

_____

4. ¿Cuál es su opinión acerca de las medidas correctivas y el régimen sancionatorio que establece la Ley Orgánica de Protección de Datos Personales?

   _____

   _____

   _____

5. ¿Considera que el tiempo establecido por la Ley Orgánica de Protección de Datos Personales para que empiece a operar el régimen sancionatorio es el adecuado?

   _____

   _____

   _____

GRACIAS POR SU COLABORACIÓN