Universidad de Cuenca

Facultad de Jurisprudencia y Ciencias Políticas y Sociales

Carrera de Derecho

Protección jurídica, Habeas Data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales

Trabajo de titulación previo a la obtención del título de Abogada de los Tribunales de Justicia de la República y Licenciada en Ciencias Políticas y Sociales

Autor:

Silvia Roxana Cordero Alemán

Director:

Diego Francisco Idrovo Torres

ORCID: 0000-0003-4833-490X

Cuenca, Ecuador

2023-11-07

Resumen

En el contexto ecuatoriano se hizo evidente la facilidad de la vulneración de la privacidad de los datos personales a través de la filtración masiva de la información de entidades públicas y privadas lo que derivó en la necesidad del planteamiento de una ley específica para su protección. Tal situación no es algo fácil, y es que pocos países han logrado hacerlo con eficacia, por lo que se planteó a través de esta investigación analizar la protección jurídica, Habeas Data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales. El estudio se desarrolló en base a los fundamentos del Derecho Comparado y se llevó a cabo un análisis de información concerniente a leyes y tratados que versan sobre la protección de datos personales fundamentales en la Unión Europea y Estados Unidos. Se concluye al respecto que en Ecuador apenas se inicia el desarrollo en protección de datos personales por lo que su eficacia no está dada por la existencia de una ley, sin embargo es el primer paso hacia lograr la garantía de los derechos de privacidad, intimidad, autodeterminación y protección de datos personales, entre otros derechos fundamentales y con reconocimiento constitucional.

Palabras clave: autodeterminación informática, derecho a la intimidad de las personas, derecho a la privacidad,protección de datos, protección jurídica

Abstract

In the Ecuadorian context, it became evident how easy it is to violate the privacy of personal data through the massive leaking of information from public and private entities, which led to the need to propose a specific law for its protection. Such a situation is not easy, and it is that few countries have managed to do it effectively, which is why it was proposed through this investigation to analyze legal protection, Habeas Data and the Organic Law on Protection of Personal Data against computer self-determination and the protection of personal data. The study was developed based on the fundamentals of Comparative Law and an analysis of information concerning laws and treaties that deal with the protection of fundamental personal data in the European Union and the United States was carried out. It is concluded in this regard that in Ecuador the development of personal data protection is just beginning, so its effectiveness is not given by the existence of a law, however it is the first step towards achieving the guarantee of the rights of privacy, intimacy, self-determination and protection of personal data, among other fundamental rights and with constitutional recognition.

Keywords: computer self-determination, right to personal privacy, right to privacy, data protection, legal protection

Índice de contenido

Índice de figuras

Índice de tablas

Dedicatoria

A mis padres, que son los pilares de mi vida. Gracias por estar siempre a mi lado, impulsándome alcanzar mis metas y por ser mi mayor inspiración en este camino académico y en la vida.

A mis hermanos y cuñada, quienes desde el principio creyeron en mí y me brindaron su apoyo incondicional.

A Pablo, por tu paciencia, comprensión y amor durante estos años y acompañar en todo momento con tus palabras de aliento. Mi mejor amigo y compañero de vida.

A mi sobrino, cuya alegría y energía han sido la luz que iluminó los días más difíciles.

A Gaby, mi amiga incondicional que sin importar las circunstancias siempre ha estado a mi lado.

Esta tesis está dedicada con todo mi amor y gratitud a cada uno de ustedes, porque sin su presencia y apoyo en mi vida, este logro no sería posible. Gracias por ser mi mayor inspiración y por motivarme a ser la mejor versión de mí misma.

Agradecimiento

A mis amigos que la universidad me dio: Kelly, Gustavo, Juanjo, compañeros de clases que se convirtieron en mis amigos de la vida.

Un profundo agradecimiento a mi tutor Diego Idrovo, cuya guía y orientación fueron fundamentales para la culminación exitosa de este trabajo de investigación.

Por último, quiero dedicar un agradecimiento muy especial a todos mis compañeros y amigos de la Universidad de Cuenca. Gracias por hacer de estos años una experiencia llena de aprendizaje, crecimiento y amistad. Ustedes han sido una parte esencial de mi viaje universitario.

INTRODUCCIÓN

En el año 2019 los ecuatorianos se mantuvieron alerta ante una noticia relevante que implicó la vulneración de la información de millones de ciudadanos, en los que incluyeron a menores de edad, puesto que se había detectado una filtración de datos en internet permitiendo el acceso a cualquier usuario de la red. Este suceso llamó la atención incluso del Gobierno quien reaccionó inmediatamente disponiendo supuestas acciones y medidas para remediar lo sucedido y sancionar a los responsables, pese a ello hasta la fecha no han solventado una serie de interrogantes al respecto, sobre todo el cómo una empresa del sector privado como Novaestrat accedió a bases de registros de entidades públicas entre las que figuraron el Registro Civil y el Banco del Instituto Ecuatoriano de Seguridad Social, por mencionar algunas.

Posterior a ello, en el año 2020, en pleno estado de emergencia, el propio Gobierno decretó una acción cuestionable como parte de las medidas restrictivas de aquel entonces, y es que consideró el uso de las plataformas satelitales de las operadoras móviles para monitorear la ubicación de las personas a quienes se les asignó permanecer en cuarentena por seguridad y cuya disposición era obligatoria. La intención era controlar el cumplimiento de esta medida y sancionar si la transgredían, por lo que la ciudadanía reaccionó con preocupación en cuanto dicha acción no poseía orden legal y competencia técnica, claramente no respetaba la garantía de protección de privacidad constitucional ni el amparo de la información personal en coherencia con los derechos humanos.

Por otra parte, en el diario ejercicio de las actividades ciudadanas, muchas de las empresas ofertan productos y/o servicios de diferente índole por vía telefónica, pero el individuo contactado ni siquiera conoce como su información pudo estar disponible para este tipo de ofrecimiento. Así mismo, otras cuantas solicitan información excesiva en sus registros para acceder a compras de productos y/o servicios sin estipular el uso de los datos, es decir su finalidad, a pesar de ello lo hacen con carácter de obligatorio. Esto ha provocado que cada vez sea más fácil el acceso a la información de tipo privado de los individuos y que su mal uso sea potencialmente elevado, en tal sentido se reconoce al titular con un alto grado de desconocimiento y vulnerabilidad al entregar su información a veces de forma automática y por otra a los responsable custodios de la misma y sus actitudes negligentes en la gestión y administración de los datos.

Estos hechos han representado un desafío para el derecho con enfoque en la intimidad y privacidad, siendo responsabilidad de las naciones la protección de estos aspectos a través de la instauración de leyes que otorguen las garantías para su ejecución efectiva. Es así que Ecuador decide adoptar la Ley Orgánica de Protección de Datos Personales en el año 2021 con su régimen sancionatorio vigente desde el año 2023.

Es por lo expuesto que la presente investigación considera analizar la protección jurídica, Habeas Data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales, para ello se consideran los siguientes objetivos específicos: analizar los términos seguridad jurídica, datos personales y autodeterminación informática dentro de la esfera jurídica ecuatoriana; identificar las diferencias y coincidencias sobre el avance jurídico referente a los temas de seguridad jurídica, datos personales y autodeterminación informática, frente a los modelos europeos y norteamericanos de protección de datos personales, con la legislación ecuatoriana en la acción del Habeas Data y en la Ley Orgánica de Protección de Datos; y determinar las debilidades y fortalezas en la esfera jurídica ecuatoriana respecto a seguridad informática, datos sensibles y la autodeterminación informática.

En tal sentido el trabajo investigativo se compone de tres capítulos, el primero enfocado en los argumentos teóricos de la seguridad jurídica en la protección de datos personales, así como una revisión de las normativas nacionales en protección de datos personales y definiciones conceptuales. En el capítulo siguiente se realiza un análisis legislativo comparado de los modelos de protección de datos personales de la Unión Europea, Estados Unidos y Ecuador. Finalmente en el capítulo tres se sintetizan las debilidades y fortalezas de la seguridad informática, datos sensibles y la autodeterminación informática en Ecuador.

CAPÍTULO I
1. FUNDAMENTACIÓN TEÓRICA

1.1. Seguridad jurídica en la protección de datos personales

En la actualidad, debido al avance tecnológico y la globalización, se ha hecho más probable la posibilidad de vulneración de la privacidad de los individuos y el uso indebido de sus información personal (Conde, 2016). Dicha situación representa un reto para el derecho, específicamente en el contexto de la protección de los datos personales, por lo que se ha recalcado la imperiosa necesidad de su regulación con un derecho independiente, sin embargo son pocas las naciones que así lo han podido ejecutar.

Es así que de los 194 países miembros de la Organización de las Naciones Unidas (ONU), 120 naciones cuentan con legislaciones referidas a la protección de datos personales, es decir el 61%, pese a ello más de la mitad no posee leyes especializadas para su regulación (Roldán, 2021). Inclusive el Ecuador, en 2016 se suscribe al Acuerdo Comercial Multipartes con la Unión Europea con la intención de comenzar el desarrollo en protección de datos personales, pero no es sino hasta 2019 que cuenta con una ley regulatoria de protección de datos, y recién en el año 2021 está entra en vigencia, además partir del año 2023 se comienza aplicar el régimen sancionatorio. Y es que, contar con una estandarización para proteger la información personal, representa diferentes beneficios tanto en el contexto social, económico y político en cuanto la tutea acertada de la privacidad de los ciudadanos refleja una sociedad democrática capaz de reconocer y proteger los derechos fundamentales (Piñar, 2010).

Además, implica una ventaja importante en cuanto permite que los inversionistas extranjeros tengan interés en el mercado ecuatoriano, sin embargo el no posee una ley regulatoria que permita el tratamiento de la información personal, dificulta el accionar empresarial pues deben enfrentarse a transferencias internaciones de datos y no existe seguridad jurídica para ello (Derechos digitales; APC, 2020).

1.1.1. Origen del Derecho a la protección de datos personales y el Derecho a la privacidad

El origen de la protección de datos se localiza en Estados Unidos con Warren y Brandeis en 1890 quienes escribieron un ensayo titulado "The Right to Privacy" en el cual se plantea la definición

de privacidad, entendida esta como un derecho que poseen las personas para no ser molestados, de forma que su argumento se encuentra en lo anónimo, lo íntimo, además sus bases son la independencia, singularidad, el desarrollo de la personalidad y la protección a la honra de los individuos (González, 2015).

Ya en el contexto legal, el juez Thomas Cooley, en el año 1868 emitió el primer referente legar de datos privados cuando consideró que las garantías de la tercera, cuarta y quinta enmiendas en la Constitución estadounidense se constituían en vías para proteger la privacidad individual (Cooley, 1879). A partir de ello, el Tribunal Supremo de EEUU denotó la existencia del Derecho a la privacidad, que se encuentra sobreentendido en primera enmienda en la cual se protege a toda persona ante cualquier forma de obligación legal de divulgar que se pertenece a una agrupación o instancia organizativa. Además, en la cuarta enmienda se evidencia la limitación hacia el gobierno de la no intromisión en aspectos personales, domiciliares, documentales y otros efectos de personales de los individuos y en la quinta enmienda se aborda respecto a la incriminación en contra de la misma persona o la revelación de la información personal (Saldaña, 2007).

Ya en 1905, la Corte Suprema de Georgia, aplicó jurídicamente la valía de protección de datos personales y la privacidad por primera vez, mientras que en el año 2009, en el caso Pavesick & New England Life Insurance Company se reconoció el derecho a la propia imagen y también el derecho a la intimidad de la vida privada, esto tomando en cuenta que se trataba de un derecho esencial que se presenta a partir de una ley natural. En la sentencia se expone respecto a la libertar personal abordando el derecho a la vida pública así como el derecho sucesivo de intimidad que posee el mismo grado de protección que el primero en mención y con condición de inviolabilidad (Kent, 2009). Es a partir de este momento que se comienzan a incrementos los derechos en el contexto de la privacidad y la protección de la información en los años siguientes en Estados Unidos.

Por otra parte, en Europa, hasta mediados del siglo XX, los referentes en protección de datos correspondían solamente a argumentos filosóficos en los que figuraron diferentes representantes de países como Reino Unido y Alemania esencialmente. Se destaca Reino Unido a partir del año 1961 con un proyecto de ley para regular y proteger la privacidad presentado por Lord Mancroft. Alemania en cambio inicia su accionar en la protección de los datos personales a partir de la Ley de Hesse, que se promulgó en 1970 en la cual se regularon determinados puntos referidos al

secreto en las comunicaciones o el derecho en el control de información, luego en 1977 se dio aprobación federal de la ley en contra del uso ilegal de los datos personales y la protección de la información (Parejo, 1993). Es a partir de estas naciones que las demás fueron incorporando de manera progresiva, las legislaciones en dicha materia.

En cuanto a América Latina y El Caribe, conforme lo expuesto por Enríquez (2017), son los países de Argentina, Uruguay, México, Perú y Colombia, quienes comenzaron a desarrollar normativas legales en protección de datos personales desde el año 2000, las cuales tuvieron gran influencia del derecho a la vida privada que se evidenció en Europa, pero desde la vigencia del Reglamento General de Protección de datos en 2018, la mayoría de naciones latinoamericana inician una reforma legal en materia de protección de datos y aquellos estados que no contaban los leyes, entre los que figuraban Ecuador y Paraguay, comienzan a desarrollar propuestas al respecto, convirtiendo a estos países en aliados estratégicos de la Unión Europea en este campo.

Es importante mencionar, que América Latina no se cuenta con un procedimiento para la integración jurídica en el contexto de la protección de datos, por lo que los reglamentos en cada nación pueden contener diversas variaciones. Ejemplo de lo expuesto, es el principio en la protección a la privacidad desde su planteamiento, certificación, notificación de violación de datos o las sanciones ante su incumplimiento, es así que en Brasil la multa asciende al 2% del total facturado por una empresa a diferencia del 4% que consta en el Reglamento General de Protección de datos de la Unión Europea (Enríquez, 2017).

1.1.2. Definición de datos personales

La protección de datos personales como derecho se ha consagrado recientemente y ha sido denominado de distintas formas: autodeterminación de la información, libertad informática, habeas data o informational privacy, entre otros términos que se emplean en las legislaciones. Su investigación se encuentra en el contexto de los derechos fundamentales, es decir un derecho pasivo de primera generación en el que se alude la no intrusión de terceros en la privacidad de las personas, es decir el derecho a la intimidad. Por su parte la Comunidad Europea que el dato personal es:

> Toda información sobre una persona identificada o identificable se considerará identificable toda persona, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (Comunidad Europea, 1995).

Se comprende entonces, que al hablar de protección de datos personales, se hace mención al amparo jurídico que se le concede a los individuos en relación a la recolección, almacenaje, uso, traspaso y cualquier otra acción que se realice con su información, destinado a que su gestión y tratamiento se efectúe con rectitud y legalidad, de forma que no se vulneren o perturben sus derechos consagrados en la Constitución y en las leyes (Aros, 2010).

Así, inclusive se considera una amenaza que obliga a los individuos al no ejercicio de sus derechos por el miedo a que sus acciones se registren en un sistema de datos personales y por lo tanto sean vulnerables de ser difundidos y usados en contra de ellos por entidades públicas, el poder privado o incluso por terceras personas que puedan imponer etiquetas sociales a las personas. En tal sentido, hacer mención del derecho a la intimidad ante la sociedad de la información implica que existe un potencial incremento de filtración de datos ya sea de manera directa o indirecta de la privacidad de los individuos y de su intimidad con el uso de las tecnologías de la información y comunicación (Aros, 2010). Y es que los medios de comunicación han provocado que los individuos sean más vulnerables, derivando en la necesidad de preservar su integridad y garantizar sus derechos.

1.1.3. Vulneración de los datos personales

Al hablar de vulneración de datos personales se comprende que a una persona le han violentado su información o se ha hecho mal uso de los mismos. Ante esto, es posible indicar que existe un gran desconocimiento por parte de las personas, lo que hace que el manejo de su información se torne complejo en cuanto a diario aplicaciones, páginas y diferentes plataformas solicitan datos de los usuarios e incluso los formularios se automatizan con las opciones de guardado automático, por lo que los individuos comparten sus datos en ocasiones de forma maquinal.

Es así que el mal uso de la información no sólo comprende el mal uso de la información general, sino también de datos concernientes a la vida privada de la persona, de su imagen, en tal sentido, la autodeterminación de la información protege esta información ante la intromisión de terceros,

sin embargo existe un aspecto que sigue primando en el entorno, se refiere a como los medios de comunicación digital, generalmente, transgreden la privacidad de las personas (Aros, 2010). Particularmente en el caso de Ecuador, en Código Orgánico Integral Penal (2014), en el artículo 229, se especifica lo siguiente:

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Mientras que en el artículo 178 en el que se refiere sobre la violación a la intimidad se explica que:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, 2014).

Por otra parte, en los convenios a nivel internacional la protección de datos respecto a la intromisión de terceros cuerda en su expresión tanto en el Pacto de San José de Costa Rica (1969) en el artículo 11, la Asamblea General de las Naciones Unidas de 1948 en el artículo 12 y la misma dignidad pero en 1966 en el artículo 17 que disponen lo siguiente:

- Ninguna persona podrá ser objeto de intrusiones de forma arbitraria o abusiva respecto a su privacidad, la concerniente a su familia, domicilio o sus comunicaciones, tampoco de agresiones ilícitas a su dignidad y buen nombre.
- Todos los individuos poseen el derecho de protección por parte de la ley ante estas injusticias o agresiones.

Como se expresa, son diferentes las doctrinas en las que se considera que los datos personales deben ser protegidos ante la intromisión de terceros, enunciando la esfera de protección de la

intimidad por lo que en convenios de índole internacional se garantiza su amparo así como la accesibilidad, enmienda y anulación de datos personales, manifestando que estos pueden ser obtenidos por el titular de los mismos cuando así lo desee o la ley lo consienta.

1.1.4. Enfoque de los derechos humanos en torno a la protección de datos personales

En el Sistema Universal de Derechos Humanos, el derecho a la vida privada se reconoce como derecho humano por lo que posee un alcance integral o global, por lo mismo la Declaración Universal de los Derechos Humanos (1948), el Pacto Internacional de Derechos Civiles y Políticos (1966), la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares (1990) y la Convención sobre los Derechos del Niño (1989) lo asumen de la misma forma y bajo las mismas consideraciones. También se lo reconoce en la Convención Americana sobre Derechos Humanos y en el Convenio para la Protección de los Derechos y Libertades Fundamentales. Sin embargo, no sucede lo mismo con el derecho a la protección de datos personales ya que en no existe un referente expreso sobre éste.

Al respecto, la Asamblea Parlamentaria del Consejo de Europa en el 1980 consideró pertinente establecer leyes en torno a la protección de datos personales que podían ser incluidas en la Convención Europea de Derechos Humanos como una referenciación, pero no fue viable debido a que se evaluó como inoportuno porque no se contaba con la suficiente experiencia en dicho ámbito y en ese momento se trabajaba apenas en el Convenio 108 para su aprobación, el cual se consideró un primer esbozo respecto al derecho a la protección de datos personales.

Posterior a ello se pueden reconocer otros convenios e instrumentos de índole internacional, pero con un alcance específico debido a que sólo tenían validez en determinas naciones, en los cuales si se contempló explícitamente el derecho a la protección de datos personales, estableciendo incluso su vinculación con el derecho a la privacidad. Es así que, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) destaca con las normas en protección a la privacidad y flujos transfronterizos de datos que se adoptaron en 1980 pero se actualizaron en el año 2013. En éstas se expresa la conformidad internacional respecto a las pautas generales para la recolección y gestión de la información de carácter personal con el objetivo de otorgar garantías a la privacidad pese a no posee un carácter vinculante, es de esta manera que la protección de datos personales toma un carácter instrumental que otorga efectividad al derecho a la privacidad.

De la misma manera en el Convenio 108 del Consejo de Europa (1980) en el artículo 1 expresa que indistintamente de la nacionalidad o residencia de cualquier individuo, se respetarán sus derechos y libertades fundamentales, específicamente el de la vida privada. Como se evidencia, es un instrumento vinculante, que está sujeto a la revalidación por parte de las naciones que forman parte del consejo europeo siempre y cuando se acojan y cumplan con los requerimientos del mismo.

En este punto es importante indicar que en el contexto de la Unión Europea, es en el que el derecho a la protección de datos personales alcanza su mayor desarrollo a nivel normativo, es de esta manera que la Directiva 95/46/CE plantea que:

> Las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario (Comisión Europea, 2016).

Posterior a este, en el año 2016, se adopta el Reglamento General de Protección de Datos que lo reemplaza, pero que mantiene los principios con aplicabilidad directa con la intención de impedir discrepancias entre las naciones que conforman la Unión Europea. Así se reconoce a la protección de datos personales como derecho en el Tratado de Funcionamiento de la Unión Europea y en la Carta de los Derechos Fundamentales de la Unión Europea (2000), siendo este último instrumento el que lo separa del derecho a la vida privada, estableciéndose su independencia sin perjudicar la relación existente entre los dos derechos.

El modelo europeo es por ende un gran referente para otras naciones de América que han reconocido a la protección de datos personales como derecho humano autónomo pero que posee relación con el derecho a la vida privada, por lo que es preciso asumir pautas normalizadas que superen el contexto nacional y hasta a nivel regional.

1.2. Derecho nacional y protección de datos personales

a) Ley Especial de Telecomunicaciones

En la Ley Especial de Telecomunicaciones (1992) en el artículo 14 se indica la prohibición a tercero de difundir la información de otra personas sin su autorización, al respecto se enuncia lo siguiente: “El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones”.

Es preciso considerar que las telecomunicaciones forman parte de la innovación tecnológica que favorece la transmisión y difusión de gran cantidad de información a los receptores y entre los mismos, es decir la población, de forma que la ley impide que se puedan realizar interferencias en dicha red de servicio. Es incluso factible, que en la información transferida por esta vía, existan datos personales sensibles por lo que podrían poner en riesgo la privacidad de sus titulares de ser revelados. También se debe tener presente que en el Artículo 39 de la ley analizada, se encuentra reconocida la protección de los derechos del usuario de las telecomunicaciones así como la privacidad del contenido, al respecto se establece lo siguiente:

> El Estado garantiza el derecho al secreto y a la privacidad del contenido de las telecomunicaciones. Queda prohibido interceptar, interferir, publicar o divulgar sin consentimiento previo de las partes la información cursada mediante los servicios de telecomunicaciones, bajo las sanciones previstas en la ley para la violación de correspondencia. Los operadores de redes y proveedores de servicios deberán adoptar las medidas necesarias, técnica y económicamente aceptables, para garantizar la inviolabilidad de las telecomunicaciones (Ley Especial de Telecomunicaciones, 1992).

Es de esta forma que se instituye el derecho al secreto y la privacidad en los contenidos transmitidos por lo que se requiere de previa autorización de las partes, esto se entiende como el consentimiento del titular de la información, así como por parte de quien emite el mensaje y también del responsable del servicio de telecomunicación, por lo que se deberán tomar las acciones necesarias para su protección de manera que estos datos no sean difundidos de forma indebida. Entonces, como se comprende, la Ley Especial de Telecomunicaciones no posee normativas claras respecto a la protección de los datos personales, debiendo entenderse que lo

que lo que se previene con esta medida es la privacidad de los individuos que otorgan sus datos para distintos fines como parte del contenido en el servicio de telecomunicaciones.

b) Ley de Comercio Electrónico, Firmas y Mensajes de Datos

En la Ley de Comercio Electrónico, también se menciona la protección de datos, así se puede analizar el artículo 1 en el que se plantea que:

> Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

En esta normativa se instituye la confidencialidad y discreción para los mensajes de datos en cuanto la información es transferida por medio de ellos y es de potestad de quien los emite y los recepta únicamente, por lo que no puede ser interferida o divulgada. Cualquier infracción o quebrando a la privacidad, tal como la intromisión por vía electrónica, la cesión ilícita de mensajes de datos o la transgresión del secresto profesional, serán sancionados. Es así como se otorga protección al derecho de la intimidad en la comunicación y se da garantía de la no filtración de datos sensibles en los mensajes. Incluso en el artículo 9 se expone que para el desarrollo, traspaso o uso de base de datos que han sido conseguidas por vías directas o indirectas, será necesario de la autorización de titular de las mismas, quien tendrá la potestad de elegir la información que se compartirá con terceras personas (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

Respecto al consentimiento expreso del titular es importante indicar que corresponde a la forma para darle a conocer a la parte interesada sobre el uso o transferencia de su información, pero posee una complicación referida a la recepción del mismo ya en la práctica, puesto que tiene que ser expresa y debe contener los compendios requeridos para que el titular pueda dar su consentimiento. En cuanto al proceso de recolección y uso de la información personal, es necesario que se guarden las medidas para proteger el derecho a la privacidad, intimidad y confidencialidad, que se garantizan en la Constitución del Ecuador y en la Ley de Comercio

Electrónico, Firmas y Mensajes de Datos, los mismo que se pueden emplear o transferir solamente con el permiso de su titular o por la autorización jurídica.

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002) también enuncia que no será necesario una aprobación del titular para la recolección de la información personal de fuentes que sean de acceso público en el contexto de su injerencia y cuando correspondan a individuos vinculados por relaciones de negocios, laborales, administrativos o contractuales y se requieran para el sostenimiento de las mismas o para cumplir contratos. Las fuentes de acceso al público son las que se relacionan con la función estatal por ende se comprende que el consentimiento no es requerido y se concibe que corresponden para disposición pública, sin embargo cuando pudiera presentarse el contacto con información de particulares que pudiera transgredir los derechos, es necesario que se los evalúe para otorgar garantías objetivas a los derechos de los titulares. También puede darse que el titular, luego de haber consentido que se compartan sus datos, identifique conflictos con la difusión o procesamiento, pudiendo proceder a la revocación, pero no se estipula el procedimiento para efectuarlo.

Por otra parte, en el artículo 32 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002) se menciona la protección de datos correspondiente a la organizaciones acreditadas que certifican la información, estipulando que éstas otorgan las garantías para su cumplimiento en concordancia con sus actividades y con lo determinado en el artículo 9 de la misma ley. Estas entidades se identificar como los registro públicos o cualquier organización de índole público que otorgue certificaciones, por lo que deberá considerar las debidas medidas tanto legales como técnicas para proteger la información sensible.

Mientras que, en lo que se refiere a la infracción de las normativas estipuladas en la ley, referidas a la carencia de autenticidad o fidelidad de la información, o respecto a seguridad y garantía en la confianza del intercambio de datos prometida a los consumidores, la entidad de control, es decir la Superintendencia de Telecomunicaciones, estará en la capacidad de plantear exigencias al proveedor del servicio electrónico para rectificar cualquier dato y hasta dar la orden para suspender la accesibilidad al servicio hasta que se dé cumplimiento de los requerimientos legales para continuar con la actividad.

c) Ley Orgánica de Transparencia y Acceso a la Información Pública

La Ley Orgánica de Transparencia y Acceso a la Información Pública (2004) tiene como fin el efectivizar el principio de publicidad de las acciones, contratos y gestión de las entidades estatales y las que son de financiamiento o interés públicos. Por lo tanto esta ley se aplica a las entidades que se sitúan en el contexto público así como a los individuos jurídicos cuyo accionar o participación, ya sea en parte o en su totalidad correspondan al Estado, al igual que los corporativos, fundaciones y organismos no gubernamentales que mantienen contratos con entidades públicas solamente si el fin de sus funciones es público, además los sujetos jurídicos de derecho privado que efectúan gestión pública, entre otros.

Esta ley implicó un gran adelanto para reconocer la accesibilidad a la información de tipo público como un derecho fundamental de las personas, sin embargo en la Constitución de la República del Ecuador (2008) se establece un nuevo ordenamiento social en el cual se otorga reconocimiento al derecho a la libre expresión en todas sus formas y manifestaciones, por lo que fue necesaria la adecuación y actualización de la ley de acceso a la información pública.

En tal contesto, en el año 2020, Ecuador ocupó el lugar 83 en la clasificación global del derecho a la información pública, evidenciado la necesidad de referir un proyecto de ley que se acoja a las normativas estipuladas en la Constitución y en los instrumentos de carácter internacional que han sido ratificados en el país que se refieren a la publicidad, transparencia y a la rendición de cuentas. En esta línea, de acuerdo con la Defensoría del Pueblo (2021) organismo superior en lo que respecta a transparencia, el 18% de las entidades que se encontraban en calidad de obligación de presentación del informe de transparencia para el periodo 2020 no lo hicieron, haciendo evidente la necesidad de fortalecer las competencias de la entidad rectora con la intención de que las acciones del gobierno se transparenten y así poder garantizar que los ciudadanos participen en la lucha anticorrupción.

d) Constitución del Ecuador

La Constitución de la República del Ecuador (2008) refiere sobre los derechos de libertad, en el artículo 66 diversos aspectos relacionados con la información personal, así por ejemplo en el artículo 11 indica que las personas poseen el derecho a la reserva respecto a sus convicciones por lo que no pueden ser obligador a exponer al respecto y bajo ningún concepto se pueden

establecer exigencias o hacer uso, sin el consentimiento del titular, de la información con carácter personal referida a su creencia religiosa, preferencia política, datos de salud o vida sexual, exceptuando en el contento de atención médica. En el artículo 19 en cambio se menciona que el derecho a la protección de datos personales implica que la recogida, almacenamiento, procesamiento y propagación de la información necesariamente demanda la permisión de su titular o un ordenamiento legal (Constitución de la República del Ecuador, 2008).

Por su parte, en el artículo 20, se expresa el derecho a la intimidad de la persona y su familia; mientras que en el artículo 21 se refiere al derecho a la inviolabilidad y secreto de la correspondencia tanto de tipo físico como la digital indicando que no se la puede retener, abrir o examinar, a excepción de los casos que prevé la ley con previa intervención legal y obligando a la preservación del secreto de las cuestiones ajenas al suceso que origine su indagación (Constitución de la República del Ecuador, 2008).

Así, se evidencia que en la Constitución se considera la protección en la accesibilidad, levantamiento y comunicación de los datos personales sin consentimiento del titular, es decir la intrusión de terceros en la privacidad del sujeto, identificándose la correspondencia directa entre la intimidad que se ve expuesta cuando se manipula y difunde la información sensible de una persona, justificándose la necesidad de amparo que el derecho debe otorgar a esta en los procedimientos en los que se gestiona y trata la misma en entidades de índole público y privado, indistintamente de su fin.

Además, es pertinente mencionar que en la Constitución, se hacen mención sobre los mecanismo de defensa jurídica relativos al derecho de protección de datos personales, siendo el más reconocido, el Habeas Data, estipulado en el artículo 92, en el cual se expresa lo siguiente:

> Acción de hábeas data. Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a 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. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la

> ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados (Constitución de la República del Ecuador, 2008).

Es de esta manera que el Habeas Data acoge diferentes fundamentos de la protección de datos sensibles de los individuos, como el otorgar la garantía en cuanto a calidad de los mismos, confidencialidad, aprobación para su usabilidad, entre otros, entendiéndose que se trata de la garantía más adecuada para el ejercicio de los derechos ciudadanos en relación al tratamiento de su información personal. Este no solo implica el que no se publique la información, pues también considera que ésta no sea empleada en procesos, se conserven medidas de seguridad para el mantenimiento de la calidad básica y también se dé el cumplimiento del objetivo por el que fue solicitado a su titular.

Así se procura también, la protección a la intimidad a través de permitir que el titular ejecute el derecho al conocimiento de la existencia y acceso, actualización, rectificación, eliminación u anulación de la documentación, información genética, bancos o archivos de datos e informes de éstos o de sus bienes que se encuentre registrados en instancias de orden público o privado, ya sea de manera digital o física y el fin en el que se los emplea. Se agrega que los responsables de los bancos de datos en los que existe información personal, no pueden difundirla sin permiso del titular, condicionando a los organismos públicos a tener cautela con dichos derechos y el titular pueda saber a qué se destinan sus datos. Además, permite que el individuo afectado ejerza la respectiva demanda por los daños provocados, si es que se no se mantienen las medidas de seguridad o si se llegara a divulgar la información y se vulneraran los derechos del sujeto (Vargas, 2013).

Esta garantía jurisdiccional se planteó en cuanto las personas se encuentran en riesgo de que su información personal sea manipulada a través de medios digitales, pues la gestión de ésta, en todas sus fases, se presenta con gran probabilidad de que sea de forma superficial y con baja responsabilidad, ocasionando que su difusión sea inapropiada. El Habeas Data por tanto, otorga el control y la disposición de los datos al titular de estos, a través de otorgarle la posibilidad de

que los conozca, acceda, rectifique e incluso los suprima si es que estos fueren incorrectos o falsos, además se reconoce como una garantía constitucional en cuanto salvaguarda derechos fundamentales como el de la intimidad y buen nombre a través de la protección de la información de las personas.

e) Código Orgánico Integral Penal

En coherencia con las actualizaciones en el contexto del Derecho Penal en Ecuador, es importante realizar una verificación respecto a la protección de los datos personales en dicha rama. Y es que, previamente se los consideraba en el concepto de "Los delitos contra la inviolabilidad del secreto y la correspondencia" del Código Penal Ecuatoriano, sin embargo desde el año 2014 tiene vigencia el Código Orgánico Integral Penal.

En el Código Penal (1971) se consideró que cualquier individuo que hiciera uso de un medio electrónico (sin distinción) para violentar contraseñas o sistemas de seguridad con la intención de tener acceso o conseguir datos protegidos que se guardan en sistemas informáticos, para transgredir el secreto, privacidad y reserva, o solamente por vulneración la seguridad, se lo reprimiría con 6 meses de prisión hasta un año, además de una multa con un monto entre quinientos a mil dólares (Código Penal, 1971).

En caso de que la información que se ha obtenido corresponda a seguridad nacional, comercial o industrial, el tiempo de condena en prisión será entre 1 a 3 años con una multa económica entre mil a mil quinientos dólares. Mientras que en los casos de difusión o uso fraudulento de los datos protegidos, además de los secretos de índole comercial e industrial, se sancionará con reclusión menor ordinaria de 3 a 6 años y multa económica entre dos mil a diez mil dólares. Y en el caso de que la difusión o el uso fraudulento sea efectuado por el individuo o individuos encargados de custodiar o usar legitimante la información, serán sancionados con prisión de 6 a 9 años y multa económica de dos a diez mil dólares (Código Penal, 1971).

Se evidencia que el Código Penal se centró en la protección de la información concerniente a la seguridad nacional o los secretos de índole comercial, incrementando su sanción, así mismo se acrecentaba la pena si la información resguardada era difundida por el que la consiguió de forma fraudulenta; así mismo ocurría si el encargado de custodiar los datos la difundía. Tales tipologías penales eran las únicas señaladas para los casos relativos con el acceso ilegal y fraudulento a

los datos protegidos y en esto se enmarcan los datos personales sensibles. Mientras que en el Código Orgánico Integral Penal (2014) también se otorga amparo jurídico a la información personal, así al respecto de los delitos remitidos al derecho de la intimidad personal y familiar se indica en el artículo 178 que el individuo que no cuente con la autorización legal y proceda a acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar la información personal, mensajes de texto, audio y video, información adjunta en elementos tecnológicos, comunicados privados o procedentes de otros individuos por cualquier medio, será sancionado con prisión de 1 a 3 años. Sin embargo, esta norma no se aplica a quien difunda grabaciones de audio y video en las que se evidencia su intervención personal o cuando se trate de información de carácter público como lo estipula la ley.

El Código Orgánico Integral Penal es sancionatorio para la transferencia de la información personal sin autorización del titular, permitiendo el ejercicio efectivo del derecho fundamental de la intimidad en cuanto sanciona la difusión de los datos, que puede darse de distintas maneras como la intercepción, acceso o reproducción, etc., con el objetivo de otorgar la debida protección a la información que por su condición deber ser privada. Se nota además la no sanción cuando el titular de los datos interviene en la grabación o medio que contiene la información puesto que se dispondría de sus propios datos y no habría infracción ante algún derecho. Tampoco existe sanción ante la difusión de datos públicos debido a que por su origen se comprende que son de dominio público.

f) Norma de Asequibilidad a Datos Personales de los Registros Públicos

La norma es aplicable a los datos personales en registros públicos con la intención de identificar a aquellos que son de libre acceso y los que se encuentran restringidos, además de las condiciones para acceder a los mismos, Los datos restringidos no pueden ser de accesibilidad pública y para su disposición se deben cumplir determinados parámetros, mientras que la información que si es accesible corresponde a aquella en la que la disposición legal permite su acceso con libertad. Sin embargo, por normativa general, los datos personales son restringidos, y se puede acceder a estos solamente por excepción (Dirección Nacional de Registro de Datos Públicos, 2015).

Se considera además que el titular de la información no posee limitaciones en su acceso en los registros de orden público que son gestionados por personas naturales o jurídicas, públicas o

privadas, así para acceder a la misma solo requerirá de la identificación. Enel caso de las personas naturales o jurídicas, públicas o privadas, tendrán acceso a la información personal de terceros en los casos señalados a continuación:

- Al tratarse de datos clasificados como accesibles.
- Al contarse con el permiso expreso del titular de los datos.
- Al estar expresamente permitido su acceso por la ley.
- Por orden judicial o de alguna autoridad competente para ello.
- En el caso de que las instancias del derecho público lo necesiten para el cumplimiento de sus debidas competencias o en concordancia con el objeto social para el que fueron creadas.

Por otra parte, en el caso de que la información a la que se requiere acceder fuere de índole patrimonial, el solicitante, necesariamente tendrá que presentar una justificación de los motivos para ello, así también efectuar la respectiva declaración con su información general ya sea para personas naturales y jurídicas. Mientras que en el caso de los datos protegidos por sigilo bancario y bursátil, la normativa plantea restricciones particulares ya que a esta solamente se puede acceder en concordancia con lo estipulado en la ley (Dirección Nacional de Registro de Datos Públicos, 2015).

g) Ley Orgánica de Protección de Datos Personales

El Reglamento General de Protección de Datos (RGPD), tuvo vigencia desde el año 2018 en Ecuador y se ha caracterizado por su alcance extraterritorial, es decir que tanto las instancias públicas como las privadas a nivel mundial deben acogerse a sus postulados. En tal contexto, el país aprobó la Ley Orgánica de Protección de Datos en el año 2021 con similitudes con RGPD dejando dos años transitorios para su aplicabilidad, de forma que las entidades públicas y privadas cuentan con 2 años para tomar medidas ante la misma, considerando que no sólo se trata de un tema jurídico sino de gestión fundamentalmente.

Dicha se ley se caracteriza por su marcada influencia de los postulados existentes en Europa, además de un indiscutible fundamento de garantía para los titulares de la información en cuanto defiende la protección del derecho personal y ciudadano por sobre el de las organizaciones empresariales, además da reconocimiento de aplicar de forma favorable al titular en casos de duda. Por otra parte, la responsabilidad proactiva y demostrada es el aspecto primordial en la

ley, ya que no solamente se espera un accionar precavido y oportuno por parte de las empresas al momento de dar cumplimiento con lo estipulado, sino que también sean capaces de confirmar que han implementado mecanismos para proteger la información personal que se les ha asignado.

Mientras que en términos de derechos, la ley plantea la dotación de estos como una forma de garantía en la aplicabilidad de la misma, así se considera el derecho a la accesibilidad, corrección y actualización, eliminación, oposición, portabilidad, restricción de tratamiento, consulta, educación digital y a no ser objeto de decisiones basadas solo en evaluaciones automáticas. Y en el caso de prestadores de servicios, existe una prohibición general en la que se indica que no se puede hacer uso de la información personal de los individuos para acciones comerciales que promuevas sus productos o servicios, esto lo podrán efectuar solo si poseen autorización expresa para ello.

1.3. Autodeterminación informativa

La autodeterminación informativa es entendida como una facultad soberana del individuo para ser solamente este quien ponga en conocimiento de otras personas su información. Así mismo, será el titular el que autorice a la anulación, corrección, actualización o eliminación de los datos en cuanto es la única persona que puede saber qué información es la que debe constar en un registro de información o base de datos y cuáles son los que se pueden difundir (Murillo, 2010).

En concordancia con la definición expuesta, en la Constitución de la República del Ecuador (2008) en el artículo 92 se hace mención a que el titular de la información será quien pueda solicitar al responsable, la accesibilidad a la misma sin un valor de por medio, ya sea para actualizar los datos, rectificarlos, eliminarlos o anularlos, por lo que la autodeterminación de la información se cumple en dicha disposición. Además, en relación al derecho a la intimidad, la autodeterminación informativa establece limitaciones ante terceras personas que deseen conocer de esta, y es aplicable para la información que se encuentra en archivos automáticos cuyos datos pudieren afectar la intimidad y el honor que son protegidos en la Constitución.

Por su parte la Tribunal Constitucional del Ecuador (2021) señala que la autodeterminación de la información, al partir de del derecho a la protección de los datos personales, requiere del otorgamiento de garantías para proteger la intimidad de los individuos además del ejercicio de

control sobre su información personal pese a no encontrarse en su potestad. Además, se debe mencionar que la libertad de la información es una facultad, que permite la disposición de los datos, la preservación de la identidad informática propia, lo que se comprende como el permiso, control o rectificación de la información que se refiere al titular y que permiten su identificación ante los demás.

1.3.1. Principios de la autodeterminación informativa

El principio de la autodeterminación de la información es relativamente nuevo en el contexto legal y sus fundamentos provienen de Alemania en relación al derecho a la privacidad tomando en cuenta que los derechos de la persona jurídica no sólo corresponden a los daños materiales sino también a aquellos inmateriales, es así que el derecho a la vida privada representa una forma de protección ante la irrupción de terceros en la vida de un individuo recogiendo el principio de tutela domiciliaria, imagen, agresión psicológica de otros, etc. (Adinolfi, 2017).

Por lo tanto, el derecho a la autodeterminación de la información es el resultado de la modernización social en la que la información es capaz de perjudicar en igual medida que una agresión física. Pero el factor que caracteriza a este derecho es la libertad del consentimiento, la posibilidad de la autorización, el bloqueo, la oposición, ratificación e incluso la indiferencia ante la información circulante del individuo (Adinolfi, 2017).

En el caso de Estados Unidos, el derecho a la privacidad se planteó como parte del principio de la tutela de la personalidad la cual enfatizaba ya sea en la identidad personal y el tutelaje de la intimidad o en el de la propiedad y en la capacidad de disposición con la aprobación (Montalbano, 2019). En este contexto el derecho a la personalidad se compuso de elementos y componentes de índole personal así como la libertad de elegir con independencia sin riesgo de ser influenciado por cuestionamientos del entorno. Tal principio como base en ciertas relaciones sociales ha tenido importancia de índole interpretativo y pudo ejercer influencia en el desarrollo de otras normativas (Palop, 2017).

1.3.2. Excepciones al derecho de protección de datos

Al igual que otros derechos de carácter fundamental, la protección de datos personales, posee excepciones que se establecen en la ley, es así que en el artículo 52 de la Carta de los Derechos

Fundamentales (Unión Europea, 2000) existe el reconocimiento a las limitaciones del ejercicio de los derechos, esto siempre y cuando estas restricciones se encuentren contempladas legalmente, acaten el contenido fundamente de los derechos y libertades y, en coherencia con el principio de proporcionalidad, sean requeridos y atiendan de forma efectiva a objetivos cuyo alcance sea de índole general y se los reconozca en la Unión Europea o solventen las necesidades de protección de los derechos y libertades de otras naciones.

Al respecto, la mayoría de las excepciones que se pueden observar en las normativas relativas con la protección de la información personal se fundamentan en el interés común ante al individual, ejemplo de ello es la defensa del Estado, temas de seguridad nacional, la protección de derechos y libertades a terceras personas o en el seguimiento ante contravenciones de tipo penal o administrativa (González, 2015).

1.4. Derechos fundamentales de privacidad e intimidad

El derecho a la privacidad e intimidad, al igual que el los derechos al honor y el de la propia imagen son reconocidos como fundamentales de los individuos, por lo mismo éste tiene derecho a reclamar su amparo para el cumplimiento adecuado y justo del derecho a la vida lo que implica por ende el derecho a que una persona sea dejada en tranquilidad. Es así que el derecho a la privacidad e intimidad permiten que se desarrolle el cumplimiento de otros derechos, por lo mismo se los considera de origen esencial e innato, extrapatrimonial, intransmisible, oponible, irrenunciable e imprescriptible y también intransferible (Pfeffer, 2010).

Es importante analizar que la intimidad o privacidad, en términos conceptuales no posee un planteamiento doctrinario y ni en la legislación se lo delimita con precisión y uniformidad. Se reconoce lo íntimo como lo que se encuentra en el interior de la persona, en los más profundo, de forma que en la modernidad, la intimidad del individuo se ve amenazada constantemente debido al gran avance tecnológico y de la comunicación digital (Tapia et al., 2021). En este contexto, reconocer la privacidad como un derecho fundamental y con afirmación constitucional se considera tardío en el orden jurídico.

Al respecto, Guzmán (2017) expresa que la concepción de vida privada implica un contexto de la vida de las personas que se debe excluir de la intromisión y difusión externas. Ante ello no es fácil el establecimiento de limitaciones precisas para determinar cuándo se está invadiendo la

intimidad o privacidad y cuando comprende un suceso que puede ser catalogado como de la vida pública. Es por ende, competencia de la justicia el establecer el contexto específico de estos aspectos en cada caso y conforme las situaciones. Sin embargo, es posible plantear algunos criterios que implican la privacidad, así se lo encuentra en el planteamiento doctrinario italiano en el cual se expone que se refiere a la soledad que imposibilita físicamente el contacto material; la intimidad en la que la persona, sin estar aislada, se incluye en un conjunto pequeño en el que se producen relaciones específicas, ejemplo de ello es el contexto de la familia o con el conyugue; también se considera al anonimato; y la discreción o reserva que implica el desarrollo de limitaciones de tipo psicológico ante las intrusiones no esperadas. De tal manera que se consideran como agresiones a la privacidad los siguientes:

- La intrusión en la soledad de tipo físico que el individuo procura en el contexto de su hogar o con sus bienes, por medio de micrófonos o cámaras que son instaladas para la grabación de diálogos privados, filmaciones en su intimidad y con su entorno.
- Divulgación pública de sucesos de tipo privado, incluso si estos no atentan al honor o no son dañinos para el individuo.
- La difusión de sucesos falsos respecto a un individuo, ejemplo de ello es la distorsión de la imagen o la voz con intenciones de comercialización.
- En la apropiación indebida para el aprovechamiento del nombre o imagen de otros.

Además, en algunas naciones se ejercen sanciones a las transgresiones a la vida privada tomando en cuenta el sitio en el que ocurren los sucesos, o también de acuerdo a la calidad personal del individuo, reconociéndose a la notoriedad como el límite concluyente entre lo público y privado, salve las acciones de intromisión en hechos expresamente privados, mientras que los países que se acogen a un sistema mixto, sancionan en conformidad del lugar y de acuerdo con la naturaleza de la acción.

1.4.1. El derecho a la intimidad enfocado a la protección de datos personales

En los Estados en los que los derechos son reconocidos a nivel constitucional, se considera la necesidad de su tutela permanente, así sucede con el derecho a la intimidad y privacidad de los individuos, puesto que se los protege de la intromisión de terceros entre los que se incluye al propio Estado, es decir que ni éste puede ir más allá de los límites de tutela y garantía. Es de esta forma que se procede a la protección total de los derechos a la protección de datos

personales que poseen los individuos ante las intromisiones a su privacidad (Ortega y Zamora, 2020). En este contexto se plantea que la información personal posee la condición de íntima por lo que está relacionada únicamente y de manera exclusiva con su titular.

Ante ello, el Estado tiene la responsabilidad de otorgar protección constante al derecho a la intimidad, más aún si se toma en cuenta que el desarrollo de la tecnología ha puesto a disposición de las personas, herramientas para transgredirlo. Es así que al incorporar leyes para garantizar la protección de los datos personales, permite que se cuente con alternativas para su defensa, además de cauciones de los derechos. De esta manera, la Corte Constitucional del Ecuador (2020) ha manifestado que “la información objeto de hábeas data es aquella relacionada con datos personales y/o informes sobre una persona o sus bienes, que reposen en instituciones públicas o privadas, en soporte material o electrónico”.

Analizado dicho argumento, se comprende que como primer elemento se encuentra el dato personal, correspondiente a toda información de carácter objetivo o subjetivo, sea esta cierta o no, relativa a un individuo. Los datos personales implican información concerniente a la vida privada y pública de un sujeto. Como segundo componente se identifica su conceptualización en la que se explica que esta información corresponde a la vida de una persona. Por lo tanto en la sentencia No. 1868-13-EP/20 se especificó que los datos personales implican información sensible relacionada con la vida privada y familiar del individuo así como cualquier acción llevada a cabo por éste independientemente de la posición que ocupe o de sus capacidades. Es por lo mismo que en se indicó que el dato personal comprende amplitud de consideraciones, por lo que la garantía de protección, el hábeas data también debe poseer extensión en su cobertura. Esta condición se comprende en cuanto todo dato que se relaciona a un individuo, lo hace identificable (Corte Constitucional del Ecuador, 2020).

CAPÍTULO II

2. ANÁLISIS LEGISLATIVO COMPARADO DE LOS MODELOS DE PROTECCIÓN DE DATOS PERSONALES

2.1. Modelo centralizado de protección de datos personales de la Unión Europea

Son muchas las naciones alrededor del mundo que han ido incorporando en sus legislaciones el tratamiento jurídico del procesamiento de datos personales a partir de la mitad de la década de los setenta y con mayor énfasis en Europa por medio de leyes y reglamentaciones, mientras que en Estados Unidos se implementó una ley sectorial (Ver figura 1).

Figura 1

Protección de datos personales en el mundo

Fuente: ANDA, 2020.

En el caso de Latinoamérica, fundamentalmente en Colombia, la regulación para el tratamiento de la información personal se fundamenta en los principios planteados por la Unión Europea que refieren el amparo del derecho a la privacidad, la autodeterminación informativa, el libre desarrollo de la personalidad, la libre expresión e iniciativa privada, esto en el contexto de garantizar los derechos humanos. Pero también hace un reconocimiento al favorecimiento

económico y seguridad social que otorga la tecnología e innovación de las empresas (Galvis, 2019).

Además, con la finalidad de dar protección a la familia, el ordenamiento político y económico se establece el amparo del derecho a la privacidad indicándose que todo individuo posee el derecho a que si vida privada y de carácter familiar, domiciliar y correspondencia sean respetados, y que no existirá intrusión por parte de la autoridad pública para el cumplimiento de dicho derecho a menos que la ley lo prevea y establezca medidas, que en un contexto social democrático, sea considerado necesario para la seguridad nacional, pública, económica, resguardo del orden y precautelación del delito, el amparo de la salud o moral o ante la defensa de los derechos y libertades de otros (Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 1950).

Entonces, al respecto, la Unión Europea ha planteado diferentes normativas para la protección del derecho a la privacidad entre los que se encuentran los siguientes:

- Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal que data del año 1981.
- Carta de los Derechos Fundamentales de la Unión Europea en el año 2000.
- Protocolos adicionales al Convenio 108 del Consejo para proteger a los individuos ante el tratamiento automático de la información personal relativa a la cesión de los datos que se registran entre 2001 hasta 2018.
- Reglamento del Parlamento Europeo y del Consejo que se registra en el año 2016, que alude el ampara de individuos en relación a la información personal y la libre circulación de esta, se enfatiza en la protección de la información personal de los niños.

De estos instrumentos, el Convenio 108 es uno de los más relevantes debido a su carácter proteccionista de los individuos en relación a la gestión de la información de índole personal, este fue una de las primeras normas que se aplicaron de forma puntual con el objetivo de otorgar las garantías respecto al derecho a la vida privada y a la libre información de todas las naciones, además enunció la definición de calidad de datos en un contexto de legalidad, rectitud y justicia, que en la actualidad se proclama a nivel nacional e internacional por el interés superior de defensa y seguridad estatal. Es así que en el Convenio 108 se estipula que la información de orden personal que sea de gestión automatizada será obtenida y tratada de forma honrada y

legítima; se la registrará con fines específicos y legales, no se la empleará para otros fines; será adecuada, pertinente y no excesiva en coherencia con los fines para los que se la registró; será exacta y de ser requerido, actualizada; se la conservará de manera que pueda ser identificada por los individuos concernidos por un plazo de tiempo que no supere el necesario para los fines de su registro (Consejo de Europa, 1981).

Ya en el año 1995, la Directiva 95/46/CE se plantea la protección de individuos físicos en el contexto del tratamiento de datos y su difusión transfronteriza en entornos cerrados, en el que las personas afectadas no suelen conocer respecto a la gestión de sus datos personales y por ende son necesarios más mecanismos de seguridad de la información y también compromiso de parte de los distintos operadores, además de exigir que sea legal la autorización del interesado independientemente del nivel de sensibilidad de los datos (Comisión Europea, 1995).

Adicional es lo expuesto, se consideró pertinente la adaptación de un proceso legal conforme el consentimiento de los niños, esto en vista de que cada vez más se emplean los dispositivos tecnológicos y las comunicaciones digitales por éstos, siendo vulnerables debido a su edad y restringida compresión del entorno digital además del incentivo a su continua participación en este mundo. Entonces en la incorporación de este proceso ajustado a los niños, se requeriría en primera instancia que se les consulte a los representantes legales previo a dar su autorización, luego se obtendría la autonomía del niño, al mismo tiempo que la de su representante legal y en el caso de los adolescente, el consentimiento único de estos (Galvis, 2019).

En otro escenario relativo a la protección de datos, los sujetos responsables de su tratamiento están obligados a otorgarle a su titular, la información que éste requiera sobre sus datos ya la finalidad de los mismos, con el objetivo que pueda decidir en base a este conocimiento. Ahora bien, el desafío es la adaptación de lo expuesto en una terminología y lenguaje apropiado a la edad de los niños en conformidad con si grado de madurez y entendimiento. Frente a esto, la Comisión Europea (1995) vislumbró más limitaciones en la accesibilidad y abastecimiento de la información como el fin del tratamiento, identidad y los datos para contactarse con el responsable de su gestión. También se estableció la probabilidad de que la parte interesada requiera la supresión de la información y el ejercicio de impedir el improcedente tratamiento de datos que permiten identificar a un individuo en entornos físicos y digitales en conformidad con las garantías de los derechos fundamentales y que se visibiliza en el contexto del derecho al olvido.

Posterior a ello, en el 2009, la Comisión Europea, inicia el procedimiento para la reformación del modelo vigente en protección de datos tomando en cuenta que se han suscitado transformaciones tecnológicas importantes por lo que se deben ajustar los principios a estos escenarios, además de procurar una mayor armonía para el potenciamiento del mercado interior. Así es como surge un reglamento para la regulación del tratamiento de datos personales por parte del sector empresarial y las instancias de gobierno en sus procedimientos diarios, el cual relaciona de forma directa a todas las naciones que conforman la Unión Europea y se caracteriza por su directa aplicación a estos.

2.2. Modelo de protección de datos personales en Estados Unidos de Norteamérica

En Estados Unidos, la protección de los datos personales está caracterizada por poseer prerrogativas en seguridad pública y defensa nacional, por lo que son necesarias medidas y juicios para retener y acceder a los datos por medio de normativas concretas. Esto quiere decir que su atención se centra en la accesibilidad a la información personal a través de las entidades de control y vigilancia con el objeto de prevenir potenciales transgresiones e inseguridades externas o propias del poder estatal. Es así como se han reconocido distintas herramientas para la regulación en conformidad con el sector social, económico y político relevantes en Estados Unidos, siendo una sociedad caracterizada por el consumismo y en la relevancia de la privacidad es ponderada por el interés superior de la seguridad y predominio de la nación (Enríquez, 2019).

Entonces, el tratamiento de los datos personales es protegido con el derecho de la privacidad. Siendo además, el derecho a la privacidad de los niños en el contexto del desarrollo de las tecnologías y comunicaciones, uno de los que posee regulación sectorial y que se aborda con especial atención por las leyes estadounidenses. Al respecto en el siglo XVIII los Estados Unidos inician el abordaje de la intimidad familiar que se relaciona con la inviolabilidad domiciliar y fija limitaciones en su accesibilidad de manera arbitraria.

Posterior a ello, en el siglo XX, se reconoce la protección de datos de forma general y en 1998 se presenta la Ley de Protección de la Privacidad en Línea de Los Niños (COPPA), con carácter sectorial se enfoca en proteger la privacidad de los datos personales de los menores y se constituye en un instrumento de referencia para otras naciones. En esta la ley se define a la información personal como aquellos datos que permiten la identificación o contacto con una persona, mientras que la recolección de la información se refiere no solamente al requerimiento

de los datos personales sino a otorgar la posibilidad de que se puedan hacer públicos por medio de ficheros como las cookies, pues esto implica el que se los pueda compartir, comercializar, etc., así como dejarlos a disposición pública en un chat, anuncio, etc. (COPPA, 1998).

Estados Unidos también recibió la Decisión de Ejecución del Parlamento Europeo y del Consejo por poseer un nivel apropiado para el tratamiento en la protección de datos, además se le otorgó el Escudo de la privacidad en el que se mencionan los principios de la privacidad y las responsabilidades y compromiso de los mandos de estadounidenses (Comisión Europea, 2016).

También, se aprobó la California Consumer Privacy Act (CCPA) en el año de 2018 y está vigente desde el 2020 en el estado de California, se trata de una ley con carácter territorial restringido, es decir que se aplica solamente a los residentes consumidores de dicho estado incluyendo personas físicas y jurídicas, e incluye a todos los operadores económicos que traten con datos personales y residan en este estado, sin embargo no a todos se los puede sancionar pues existen determinados juicios económicos que se establecen en esta ley. En general su objetivo es el poder controlar de forma más efectiva a los consumidores respecto a la información personal que es recolectada por los distintos operadores económicos.

Además, a partir de COPPA (1998) se identifican 4 derechos que no se había reconocido en Estados Unidos en cuanto a protección de datos personales, estos comprenden el derecho del consumidor al conocimiento de toda su información personal recopilada; el derecho al conocimiento de cómo se efectúa el tratamiento de su información personal; derecho a eliminar los datos personales recolectados por las entidades; y finalmente el derecho a la no discriminación de las empresas (Becerra, 2020).

También es importante tener presente que esta ley no posee un principio de finalidad y estándar, solamente plantea determinadas condiciones pues resulta obligatorio para las empresas, el reconocer categorías para cada uno de los datos personales que se recopilan, haciendo mención a las fuentes empleadas en la obtención de los mismos, así como su finalidad comercial o empresarial y quienes son los terceros con los que se compartirá dicha información (Jehl y Friel, 2018). Sin embargo, el no contar con un principio rector y un estándar para limitar el tratamiento de los datos a un fin específico podría ocasionar que se presenten intrusiones e infracciones en la privacidad del consumidor.

2.3. Tratamiento de los datos personales en Ecuador

En Ecuador no existía una ley para para delimitar el ejercicio y regulación del derecho de la protección de datos personales, sin embargo la necesidad de este fue latente cuando se suscitaron hecho de carácter público que denotaron la vulneración de la información de las personas, uno de ellos se presenta en 2019 cuando se identifica una filtración masiva de datos personales sensibles de los ciudadanos ecuatorianos que incluyeron a menores de edad y a los que cualquier usuario en internet podía acceder, se estimó que se trataron de 20.8 millones de registros en los que se podía encontrar información de carácter personal así como relativos al entorno laboral, propiedades, comportamiento bancario, etc. (El Telégrafo, 2019).

Luego en el año 2021, mientras transcurrió la pandemia, se presentó otra filtración que involucró a una entidad pública, el Ministerio de Salud Pública del Ecuador, que también sufrió una gran filtración de información de los pacientes a nivel nacional en los que constaban nombres, apellidos, tratamiento recibido, pacientes fallecidos, etc., información que se podía visibilizar en internet (Fundamedios, 2023). En el mismo año, el Banco del Pichincha, enfrentó un ataque de seguridad que comprometió sus registros de información aunque no se dio mayor explicación del hecho, puso en riesgo la confianza en la entidad así como la tranquilidad de sus clientes (Díaz, 2021). Además de estos hechos, el último registrado fue en el año 2023 cuando nuevamente el Ministerio de Salud Pública se vio involucrado en un caso de filtración de datos, pues un hacker indicaba contar con datos de vacunación de Covid-19 de la población ecuatoriana que los ponía a la venta con información de números de cédula de ciudadanía, e-mail, números telefónicos, etc. (Díaz, 2023).

Estos son solo algunos casos, pues no todos son públicos, además existe una vulneración a los derechos de protección de la información personal que se puede evidenciar en acciones diarias como en las compras digitales en las que se registra información y por otra parte la venta de bases de datos es común en distintas plataformas en las que se ofertan registros actualizados de entidades como el Consejo Nacional Electoral, el Registro Civil, etc. (Fernández et al., 2022). Sobra decir, que en la mayoría de los casos, la recolección de la información y su posterior comercialización no posee autorización.

Es justamente por lo expuesto que en Ecuador se hizo cada vez más relevante la necesidad de incorporar un instrumento legal para estandarizar la protección de la información persona y

regular apropiadamente el consentimiento por parte del titular de la misma, así como el tratamiento de esta. Es así que en los ejes estratégicos del Plan Nacional de la Sociedad de la Información y el Conocimiento 2018-2021 se planteó la promulgación de una ley orgánica de protección de datos personales para la regulación y amparo en la ejecución del derecho a la protección de datos personales.

Es así que entra en vigencia en el año 2021 la Ley de Protección de Datos Personales y si régimen sancionatorio en el año 2023. El objetivo de esta ley es el regular el accionar del derecho a la protección de datos personales y autodeterminación de la información a través de normas, derechos, obligaciones y mecanismos para su amparo, por lo se requiere que las empresas a nivel nacional, sean estas públicas, privadas y sin distinción de su actividad económica o tamaño, efectúen un reconocimiento de los datos personales que gestionan, los contextos en los que se plasman y que lleven a cabo un análisis del proceso que ejecutan con estos, todo ello con la intención de comprobar si lo están llevando a cabo en coherencia con las disposiciones legales y sus fundamentos.

Por lo mismo, en un primer momento, las empresas ecuatorianas gozaron de un periodo de adaptación comprendido en un lapso de 2 años, tiempo en el cual debieron proceder con la implementación de los parámetros establecidos en la ley de forma apropiada, tomando conciencia de sus obligaciones ante los titulares del derecho. La Ley de Protección de Datos Personales se encuentra fundamentada en los principios europeos y se divide en 12 capítulos, además plantea la creación de una Superintendencia de Protección de Datos encargada de la rectoría en el cumplimiento de la ley, así mismo se propone el desarrollo del reglamento para su ejecución, sin embargo ninguno de estos dos aspectos se ha ejecutado aún.

Por otra parte, la ley contiene los principios estratégicos para llevar a cabo su acatamiento, siendo estos el de seguridad que mencionar la necesidad de incorporar medidas para evaluar y actualizar los procesos en la recolección de la información, además está la proporcionalidad que se refiere al requerimiento de datos necesarios por parte de las entidades, adicional a ello se suman los principios de justicia, lealtad, confidencialidad, calidad, conservación, entre otro (Ley Orgánica de Protección de Datos Personales, 2021).

Mientras que el régimen sancionatorio establece multas económicas, están van desde la consideración de leves hasta aquellas consideradas graves, aplicables a los responsables de las

gestiones de los datos personales, además de los encargados. Las sanciones establecidas oscilan entre el 0,1% al 1% del total del volumen del negocio y los causales para su ejecución son diversos, siendo los más relevantes por el contexto de los análisis efectuados en los casos ecuatorianos, el no atender requerimientos de los titulares o realizarlos en periodos de tiempo no establecidos, otorgar la gestión de los datos a quien no pueda dar las garantías necesarias para hacerlo de manera adecuada, emplear la información recolectada para otros fines diferentes a los que han sido declarados, no poseer normativas técnicas u organizativas para el tratamiento de la información, entre otros.

Así se puede expresar que la Ley Orgánica de Protección de Datos Personales (2021) se ha desarrollado con la finalidad de otorgar amparo a los derechos de los individuos, incluyendo el derecho de privacidad, autodeterminación informativa y libertad personal. Constituyéndose en un instrumento de gran relevancia y beneficio para el Ecuador, pues permitirá el conveniente trato de la información siendo viable para los inversionistas del exterior y la mejora en los servicios digitales, con esto también se previene la filtración de información de las entidades de carácter público y privado, y las violaciones a los derechos de los titulares de la misma, como ha venido sucediendo.

2.4. Diferencias y coincidencias sobre el avance jurídico en seguridad jurídica, datos personales y autodeterminación informática

Una vez efectuada la revisión del sistema normativa europeo, estadounidense y el ecuatoriano es importante efectuar un análisis comparado, así en el Reglamento General de Protección de Datos desarrollado en Europa, se puede evidencia un nivel de protección elevado, en este caso la autorización por parte del titular es la base para la legitimación del tratamiento de datos aunque también se presentan otras formas de legalización. Se destaca también la existencia de una autoridad encargada de custodiar el cumplimiento de la ley en cada nación con el fin de que no se vulneren los derechos fundamentales.

En el caso de Estados Unidos, no se cuenta con una ley federal para la regulación y protección del derecho a la protección de datos, más bien se plantea que los titulares de la información sean quienes autorregulen este derecho y de ser vulnerado se acudirá al sistema judicial para requerir el resarcimiento por los daños y perjuicios. Se destaca la ley COPPA en la cual se consideran algunos fundamentos del reglamento europeo y se da vida a cuatro derechos que antes no se

contemplaban en el sistema, pese a ello esta normativa aún representa un estándar básico en la protección de la información.

Mientras que en Ecuador, se incorpora la Ley Orgánica de Protección de Datos Personales en el año 2021 y es con la misma que se logran la delimitación conceptual de protección de datos, se establecen los principios para su aplicación, así como se instituyen los derechos de los titulares de la información y las obligaciones de quienes actúan como responsables en el tratamiento de la misma. Se puede observar que el consentimiento es una de las formar de legalizar el tratamiento de la información y el cual posee una estandarización de amparo a detalle y de forma específica.

Tabla 1

Estándares en legislación comparada

Consideración	Reglamento General de Protección de Datos Personales	California Consumer Privacy Act	Ley Orgánica de Protección de Datos Personales
Forma de legitimar	Son 6: consentimiento como regla general.	No existen exigencias legales.	Son 7: consentimiento es una de las formas.
Características	Son 4: libre, específico, inequívoco e informado.	Sistema opt out, sistema de exclusión en la venta de datos personales.	Son 6: libre, previo, específico, expreso, informado e inequívoco.
Finalidad	Son 3: determinada, explícita y legítima.	No existe estándar.	Son 3: determinada, explícita y legítima.

Fuente: Roldán, 2021.

Ante lo expuesto, se puede evidenciar que el orden jurídico en Ecuador, procura la alineación con el estándar de la Unión Europea, a pesar de ello posee variaciones importantes que solamente podrán evaluarse cuando la ley sea ejecutada. Es así, que, para que Ecuador cuente con un nivel apropiado de protección de datos debe cumplir con tres aspectos, el primero es contar con una norma que otorgue las garantías necesarias para el cumplimiento de este derecho, el segundo es que exista una autoridad de Estado lo suficientemente competente e independiente para velar por su cumplimiento, y el tercero es posee una normativa especializada en la materia (Serrano, 2022).

Frente al planteamiento expuesto, la ley vigente se constituye en la norma especializada en la protección de datos, siendo su fin “regular el ejercicio del derecho a la protección de datos

personales, la autodeterminación informativa, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela" (Ley Orgánica de Protección de Datos Personales, 2021). En esta ley se contemplan todos los mecanismos para legitimar el tratamiento de la información que se establecen en el Reglamento General de Protección de Datos europeo y además adiciona dos componentes. En relación a la finalidad se mantienen las mismas especificaciones en los dos cuerpos normativos. Por lo expuesto es posible indicar que la ley ecuatoriana se vislumbra como un modelo sólido, inclusive en algunos puntos resulta más exigente que el reglamento europeo.

Por otra parte, la efectividad de ley es un aspecto que no se puede reconocer aún, en cuanto su implementación es reciente y hablar de reformas es temprano pues se debe analizar y evaluar la aplicabilidad de la misma. En el caso de la Unión Europea en cambio, la protección de datos lleva aproximadamente cuarenta años en constante desarrollo, pero uno de los aspectos que se pueden destacar como relevantes en su modelo es la educación, para lo cual, las autoridades competentes deben priorizar en la formación y conocimiento de la ley tanto a los sujetos titulares así como a los responsables y encargados en el manejo de la información. Se considera que la existencia de una cultura de protección de datos y la concientización contribuirán a que el este derecho forme parte en la sociedad ecuatoriana. Para ello es importante realizar la debida difusión por medios de campañas, capacitaciones y sistemas de información en torno a esta materia.

Continuando con los planteamientos de Serrano (2022) el requerimiento de contar con una dignidad de estado con carácter independiente para que vele por el cumplimiento de la ley, esta será una entidad de orden público que posea independencia administrativa y financiera y que cuente con personería jurídica. No tendrá relaciones de subordinación o jerarquización con la administración central. Para ello se ha considerado en la Ley Orgánica de Protección de Datos Personales, la creación de una entidad competente para velar por su cumplimiento.

Sin embargo la tendencia en el país ha sido hacia la reducción de las dependencias estatales y es que la situación económica, social y política no presentan escenarios favorecedores para la creación de una nueva autoridad independiente, no obstante una solución viable podría ser la creación de un organismo adjunto a la Dirección Nacional de Registros Públicos, pero podría presentarse el caso de afectación en la seguridad jurídica y el desarrollo pleno del ejercicio del derecho a la protección de datos. En cuanto a las funciones de este organismo rector, la Ley

Orgánica de Protección de Datos Personales (2021) expone que le corresponden supervisar, controla, evaluar, autorizar y normar. En tal sentido, dicha entidad podría formar parte de la Función de Transparencia y Control Social, así el cuerpo colegiada se conformaría por actores de sectores como el público, privado e incluso de la academia, que se realizaría a través de su elección en un concurso de méritos y oposición, evaluando su formación educativa, experiencia profesional y la experiencia específica en la rama.

Finalmente el último punto expuesto por Serrano (2022) referido a contar con una norma estándar en protección de datos, en Ecuador si bien no se cuenta con un reglamento como la Unión Europea, se tiene un régimen sancionatorio que establece un referencial básico y un máximo que son altos en el sector privado calculados respecto al volumen del negocio correspondiente a los ingresos de la empresa previo a la conciliación tributaria. Es posible indicar que la normativa no es clara con los aspectos relativos a las sanciones por lo que se da paso a la discreción amplia de la autoridad, la cual se limitará por los principios del derecho administrativo.

CAPÍTULO III

3. DEBILIDADES Y FORTALEZAS DE LA SEGURIDAD DE LA INFORMACIÓN, DATOS SENSIBLES Y LA AUTODETERMINACIÓN INFORMATIVA EN ECUADOR

3.1. Debilidades en la protección de datos personales en Ecuador

La Ley Orgánica de Protección de Datos Personales (2021) procura garantizar de forma efectiva el ejercicio del derecho por medio de una normativa especializada. Sin embargo es preciso analizar potenciales debilidades que ésta presenta, uno de ello por ejemplo se encuentra en cómo se limita la información pública y la personal en la protección jurídica pues lo correcto habría sido el plantear la ley de protección de datos y a partir de ésta establecer en qué casos o situaciones la información personal se transforma en pública, no obstante en el Ecuador la situación se dio a la inversa.

Ahora bien, considerando lo que respecta al responsable del tratamiento de datos, su definición expresa que es quien “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” (Ley Orgánica de Protección de Datos Personales, 2021). Pero este planteamiento definitorio podría resultar inadecuado en cuanto indica que el responsable es quien decide acerca del fin y el tratamiento de la información. Y es que un administrador de bases de información no es generalmente o necesariamente quien se responsabiliza de su tratamiento, de hecho solo podría ser el encargado, pues en la modernidad, la información que se ingresa y procesa a través de los aplicativos y plataformas digitales, es almacenada en bases de datos automáticamente.

Ahora bien en lo que respecta al encargado del tratamiento de datos, comprende a un sujeto "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" (Ley Orgánica de Protección de Datos Personales, 2021). Tal definición no se presenta de manera específica respecto al encargado, se deduce una confusión en las definiciones fundamentales, en cuanto un responsable de base de datos puede serlo también en el tratamiento de la información y encargado. Su responsabilidad es recibir la permisión del titular de establecer los medios y fines para tratar los datos personales. Será encargado si efectúa el tratamiento de la información por cuenta del responsable.

En lo que se refiere a la seguridad y confidencialidad de los datos personales, en la ley no existe regulación para los seudónimos, ni el cifrado así como para la aplicación de normas de seguridad, se alude a la seguridad y confidencialidad de forma general. Y en cuanto a la autoridad responsable de la protección de datos personales esta no se ha establecido aún, pese a que la ley entró en vigencia en 2021 y se han tenido dos años para su adaptación y muchas de las disposiciones en la normativa refieren la intervención de esta autoridad. Al respecto se la define como: "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" (Ley Orgánica de Protección de Datos Personales, 2021).

3.2. Fortalezas en la protección de datos personales en Ecuador

La Ley Orgánica de Protección de Datos Personales (2021) parte de la concepción de que se trata de derechos fundamentales puesto que la protección de los datos personales es un derecho relativo a la dignidad del ser humano. Tal concepto se fundamenta en los postulados interpretativos de la jurisdicción de la Unión Europea y el Consejo, dejando abierta la posibilidad para el descubrimiento de que la protección de la información personal es algo necesario y se relaciona directamente con los derechos humanos.

Por otra parte, la ley favorece para que las personas gocen del derecho a acceder, rectificar, impedir y eliminar la información incorrecta acerca de sí mismos que se encuentre almacenada en bases de registros y que pudieran afectar a sus derechos. También otorga direccionamiento a los responsables y encargados en el tratamiento de los datos. Cabe indicar que esta ley goza de efectividad extraterritorial, por lo que si una organización situada en el exterior, es decir fuera del territorio ecuatoriano, recaba información de los ecuatoriano, deberá sujetarse a la normativa. Adicional a ello se puede manifestar que es aplicable en el sector público y privado sin distinguir el tamaño de la empresa o su rama de actividad.

También es importante valorar que la ley presta un especial reconocimiento al consentimiento por parte del titular como una forma de legitimar el derecho a la protección de los datos personales y al respecto refiere que éste debe otorgarse en libertad, especificidad, de manera informada e inequívocamente. Es decir que al individuo se le asigna la capacidad de decisión en relación a quién, cómo, cuándo y para qué se van a usar sus datos personales. Esto denota la

validez de un derecho ciudadano y fundamental en un Estado constitucional de derechos en el que existen garantías para su cumplimiento.

La normativa también efectúa el reconocimiento de distintos derechos que permiten garantizar la protección de los datos personales de una forma efectiva, uno de ellos es el derecho a la información sobre lo que se va hacer con la información, el tiempo de preservación, quien será el responsable de su tratamiento y las consecuencias de su uso. También se establece el derecho a no ser objeto de decisiones fundadas solamente o de forma parcial en consideraciones automáticas, de esta manera se protege al titular de potenciales arbitrariedades ante sus derechos y libertades fundamentales por el desarrollo de perfiles.

En el caso de los niños y adolescentes, la norma da reconocimiento a su derecho de protección de datos desde un enfoque garantista, así se reafirma que al ser un segmento vulnerable, requiere de acciones de amparo especializadas. Además, la ley incorpora el derecho a la educación digital de las personas, esto permite que se fomente el uso apropiados de las tecnologías de la información y comunicación y contribuye en la reducción de las diferencias socioeconómicas de la nación. Otro aspecto importante es que la ley da reconocimiento a cuatro clases de datos personales, siendo su tratamiento indebido o restringido, esta tipología incorpora a información sensible en la que se considera a individuos fallecidos e información crediticia, datos de la niñez y adolescencia, referentes de la salud y de individuos con discapacidad. Estos datos están limitados o prohibidos según sea el caso porque pueden afectar de forma directa en la intimidad de la persona o repercutir en el cumplimiento de otros derechos con carácter fundamental.

La ley también limita la posibilidad de que la información personal sea transferida con intenciones que puedan vulnerar los derechos de los titulares y por ende transgredan sus derechos e integridad, para ello se requiere del consentimiento y también de la información de lo fines legítimos del uso de la información. Adicional a esto, plantea quince obligaciones para el responsable y el encargado del tratamiento de la información personal entre los que figuran el hacer uso de procedimientos e instrumento legítimos y legales, incorporar sistemas de valoración y comprobación para los sistemas de tratamiento y seguridad, plantear políticas para prevenir riesgos y amenazas, etc. Es mediante estas acciones que se plantean las responsabilidades de quienes pueden acceder y controlar la información personal.

3.3. Consideraciones generales

Es claro que el derecho a la protección de datos personales es una respuesta al desarrollo de las tecnologías de la información y comunicación y la modernización, por lo que cada vez más es importante proteger de forma eficaz e integral la información de índole personal. Frente a esta realidad, las naciones como Ecuador deben plantear la adopción de mecanismos preventivos y tutelares para la vigencia efectiva de los derechos que se derivan del derecho a la protección de datos. Es así que las políticas públicas deben orientarse a la adecuada prevención y adquisición de conciencia en torno al uso y tratamiento apropiado de datos, con la intención de redirigir y propagar una cultura segura y respetuosa ante el derecho al protección de datos.

La garantía del derecho en mención implica que se cuente con políticas públicas que permitan efectivizar los derechos en coherencia con la dignidad humana y permitan que se adquiera conciencia y se pueda educar a las personas respecto a los conflictos que ocasiona el difundir datos sensibles sin la autorización de su titular. Además, la seguridad de la información implica confidencialidad, honradez y la disposición de los datos por medio de la incorporación de sistemas de seguridad y control necesarios y obligatorios para su protección, así se garantizan los derechos del titular.

Por lo que las empresas se ven obligadas a la implementación de medidas acordes y necesarias para el cumplimiento de la ley y por ende de los derechos que en esta se estipulan, también deberán incorporar procedimientos para monitoreas y mejorar permanentemente dichas medidas y recabar las evidencias necesarias para evidenciar su cumplimiento. En este contexto, se reconoce como vía complementaria de aplicación la normativa ISO que implica la incorporación de mejores prácticas, e inclusive la propia Ley Orgánica de Protección de Datos Personales en el artículo 37 efectúa como recomendación el poder apoyarse en estandarizaciones de carácter internacional para una apropiada gestión de los riesgos con enfoque en el amparo de los derechos y libertades. La norma ISO aborda la seguridad de la información de manera ampliada y ofrece una normativa detallada en protección de datos personales ajustada al contexto ecuatoriano.

CAPÍTULO IV
4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Luego de efectuada la revisión de normativas y en concordancia con el objetivo de analizar la protección jurídica, Habeas Data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales es posibles concluir que en Ecuador pese a ser reciente la incorporación de la ley, esta se plantea bajo un esquema sólido fundamentado en el modelo de la Unión Europea, el cual se caracteriza por basar sus principios en los derechos humanos y considerar la protección de datos como un derecho fundamental.

En tal sentido la Ley Orgánica de Protección de Datos Personales se constituye en un instrumento que ha procurado abordar todos los aspectos para garantizar el amparo de la información y contempla principios importantes para su cumplimiento, haciendo énfasis en cómo se los debe incorporar y en la relevancia de su acatamiento por parte del responsable y encargado del tratamiento de los datos. Por lo que en comparación con el modelo europeo, la norma ecuatoriana es muy similar, obviamente con variaciones puntuales debido al contexto donde se aplica pero igualmente extraterritorial.

En cuanto al análisis de los términos seguridad jurídica, datos personales y autodeterminación informática dentro de la esfera jurídica ecuatoriana es pertinente considerar que estos se comprenden bajo las mismos planteamientos a nivel internacional. Es así que la seguridad jurídica se entiende como la convicción o garantía de que el orden legal sea aplicable objetivamente, se trata de un principio fundamental de un Estado de Derecho, siendo una caución que éste brinda a los individuos respecto a que sus derechos constitucionales se respetarán así como todos aquellos consagrados en las leyes, por lo que no se los vulnerará ni alterará. Mientras que el dato personal es entendido como aquel que permite la identificación o hace identificable a un individuo natural ya sea de forma directa o indirecta. En cuanto a la autodeterminación esta se reconoce como la reclamación del consentimiento del titular de la información como norma observable previa a cualquier tratamiento de la misma y que se puntualiza en la reglamentación europea como un efectivo derecho a la intimidad, propio y primordial.

Planteado esto se identifican las diferencias y coincidencias sobre el avance jurídico referente a los temas de seguridad jurídica, datos personales y autodeterminación informática, frente a los modelos europeos y norteamericanos de protección de datos personales, con la legislación ecuatoriana en la acción del Habeas Data y en la Ley Orgánica de Protección de Datos. Al respecto es posible indicar que Ecuador es una nación que apenas comienza su desarrollo en estos aspectos, pese a contar con algunos planteamientos constitucionales y leyes que han intentado el abordaje de los derechos de protección de la información personal pero no se han especializado en ello. Recién en el año 2021 la ley entra en vigencia y su régimen sancionatorio en el 2023 por lo que las empresas públicas y privadas, así como toda la población ha tenido dos años para su adaptación y conocimiento, periodo que ya ha transcurrido y a pesar de ello aún no se han cumplido todos los puntos establecidos en la norma, como el de crear una entidad rectora para velar por el acatamiento de la ley.

Al respecto el modelo europeo tiene vasta experiencia en el desarrollo de normativas en la protección de datos personales pues lleva alrededor de cuarenta años en constante actualización y reforma de acuerdo con las necesidades de la sociedad y los avances de las tecnologías de la información y comunicación. Es así que las naciones optan por tomar como referencia su reglamento por ser el más avanzado y procuran guiarse en sus acciones para logar la misma efectividad en la aplicación de sus leyes. En cuanto al modelo estadounidense, aún no se cuenta con una ley general a la que se acojan todos los estados, pero de destaca la Ley de Protección de la Privacidad en Línea de Los Niños y Consumer Privacy Act aplicable únicamente en el estado de California, por lo que se considera que aún tienen mucho camino por transitar en términos de protección de la información.

Finalmente en este escenario se determinan las debilidades y fortalezas en la esfera jurídica ecuatoriana respecto a seguridad informática, datos sensibles y la autodeterminación informática. Las primeras implican aspectos más bien de definiciones que se estipulan en la ley y que pueden estar sujetos a dudas en su interpretación sobre todo en lo que se refiere al responsable y el encargado del tratamiento de datos personales, por otra parte una de las debilidades más relevantes en la actualidad es precisamente el no contar con la autoridad rectora que se encargue de velar por el cumplimiento de la ley y es que además de ello en ésta se evidencia que posee varias responsabilidades para su efectivo ejercicio, por lo que no tener disponible aún a esta figura implica potenciales vulneraciones a sus disposiciones.

Referente a las fortalezas, la ley otorga un escenario jurídico favorecedor para los ciudadanos en cuanto a la protección de sus datos personales a través del amparo de los derechos de privacidad, intimidad, autodeterminación, entre otros. La información de niños, jóvenes y adultos ya no será usada de forma arbitraria por ninguna instancia y de hecho deberán ser resguardada bajo mayores medidas de seguridad y gestión de la misma para evitar su filtración o acceso indebido por parte de terceros. Así mismo, se plantean sanciones a los responsables y encargados del tratamiento de los datos que no cumplan con las disposiciones establecidas en la norma y que por lo mismo ocasiones transgresiones a los derechos de protección de datos personales de los titulares. Esto denota un gran avance para el país en términos de actualización legal, tecnológica y administrativa que incluso puede convertirse en una ventaja competitiva puesto que se respeta la privacidad e intimidad de las personas en concordancia con los derechos humanos.

Pero sobre todo, en un contexto social caracterizado por lo masivo, por los constantes intercambios de información, por la automatización, e incluso por la falta de atención de los propios titulares a la información que otorgan, en el que se irrespeta lo privado e incluso se lo comercializa y difunde, a veces hasta con morbo, es necesario que existan limitaciones, controles sobre los datos que pueden ser públicos, porque la privacidad de una persona es un derecho humano fundamental que se debe respetar.

4.2. Recomendaciones

En concordancia con las conclusiones planteadas se exponen las siguientes recomendaciones:

Considerando que la Ley Orgánica de Protección de Datos Personales es de reciente vigencia en el Ecuador, se deben reforzar los programas de educación e información al respecto en todos los niveles de la población, pues no sólo en el contexto empresarial público y privado. Esto se debe a que toda la población está involucrada su cumplimiento pues todos los ciudadanos, desde los menores de edad, hasta los adultos están expuestos a diario a medios a través de los cuales se otorga información automáticamente, hoy en día este comportamiento tiene que ser fundado en un conocimiento legal, debido al potencial mal uso que se puede dar de la información personal. Se trata de una responsabilidad compartida entre el titular, los responsables y encargados, así como del Estado a través de las leyes para que la protección de los datos personales sea efectiva.

También es importante evaluar el proceso de adaptación de la ley en el periodo que se ha tenido para ello, pues si bien se ha podido constatar que muchas entidades ya difunden en sus comunicados, redes sociales, páginas web y a través de diferentes medios de su acatamiento a de la ley, existirán otras cuantas aún no lo hacen por desconocimiento de cómo aplicarlo u otros motivos. En este escenario es importante continuar trabajando en la difusión y capacitación para lograr que el país se acoja a esta disposición legal y la reconozca como un proceso cotidiano.

Finalmente se sugiere la evaluación de la efectividad en la aplicación de la ley en el periodo pertinente, que si bien esta es una responsabilidad del Estado, debería serlo también del órgano rector encargado de velar por el cumplimiento de la norma, que casualmente no existe. Por lo que también es pertinente analizar por qué aún no se cuenta con esta dignidad. En tal sentido es claro que aún queda mucho por indagar en relación a la aplicabilidad de la Ley Orgánica de Protección de Datos Personales por lo que quedan aspectos que se deben continuar estudiando en lo posterior.

Referencias

Adinolfi, G. (2007). Autodeterminación informativa, consideración acerca de un principio general y un derecho fundamental. *Cuestiones constitucionales, 1*(17), 3-29.

Agencia Española de Protección de Datos. (2016). *Informe 2016 La protección de datos de los menores de edad.* Madrid: Trama Editoriales.

Aros, R. (2010). El derecho a la intimidad frente a la sociedad de informacion. *Revista De Derecho - Pontificia Universidad Católica De Valparaíso, 1*(22), 209-222. Obtenido de https://www.rdpucv.cl/index.php/rderecho/article/view/478

Asamblea General de las Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos.* Asamblea General de las Naciones Unidas. Obtenido de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Asociación Nacional de Avisadores de Chile - ANDA. (2020). *Mapa global de la privacidad de datos, por la WFA.* Vitacura: ANDA. Obtenido de https://www.anda.cl/revista/mapa-global-de-la-privacidad-de-datos-por-la-wfa/

Becerra, X. (2020). *Ley de Privacidad del Consumidor de California (CCPA).* California: Departamento de Justicia del Estado de California. Obtenido de https://oag.ca.gov/privacy/ccpa

Cimpanu, C. (2019). El nuevo ataque PDFex puede filtrar datos de archivos PDF encriptados. *ZDNET*. Obtenido de https://www.zdnet.com/article/new-pdfex-attack-can-exfiltrate-data-from-encrypted-pdf-files/?ftag=COS-05-10aaa0g&utm_campaign=trueAnthem%3A%20Trending%20Content&utm_content=5d927072b1a00400017b59c3&utm_medium=trueAnthem&utm_source=twitter

(2015). *Código Civil.* Quito: Asamblea Nacional. Obtenido de https://www.acnur.org/fileadmin/Documentos/BDL/2017/10979.pdf

(2014). *Código Orgánico Integral Penal.* Quito: Asamblea Nacional. Obtenido de https://www.funcionjudicial.gob.ec/lotaip/phocadownloadpap/PDFS/2014/Nacional/3%20Codigo%20Organico%20Integral%20Penal.pdf

(1971). *Código Penal.* Quito: Asamblea Nacional. Obtenido de https://www.oas.org/juridico/PDFs/mesicic4_ecu_penal.pdf

Comisión Europea. (1995). *Dictamen 4/2007 sobre el concepto de datos personales. Grupo de Trabajo del Artículo 29.* Bruselas: Directiva 95/46/CE. Obtenido de

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Comisión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.* Bruselas: Directiva 95/46/CE (Reglamento general de protección de datos). Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Conde, C. (2016). *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad.* Cádiz: Dykinson. Obtenido de https://rodin.uca.es/handle/10498/26396

Consejo de Europa. (1980). *Convenio 108 del Consejo de Europa.* Estrasburgo: Consejo de Europa. Obtenido de https://www.oas.org/es/sla/ddi/docs/Convenio_108_CE.pdf

Consejo de Europa. (1981). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* Estramburgo: Consejo de Europa. Obtenido de https://www.boe.es/eli/es/ai/1981/01/28/(1)/dof/spa/pdf

(2008). *Constitución de la República del Ecuador.* Quito: Asamblea Nacional del Ecuador. Obtenido de https://www.cec-epn.edu.ec/wp-content/uploads/2016/03/Constitucion.pdf

(1998). *Constitución Política de la República del Ecuador.* Quito: Asamblea Nacional. Obtenido de https://www.cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_1998.pdf

(1984). *Convención Americana sobre Derechos Humanos.* San José: Conferencia Especializada Interamericana sobre Derechos Humanos. Obtenido de https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

(1990). *Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares.* Resolución 45/158 de la Asamblea General. Obtenido de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers

(1989). *Convención sobre los derechos del niño.* Asamblea General de las Naciones Unidas. Obtenido de https://www.un.org/es/events/childrenday/pdf/derechos.pdf

(1950). *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.* Roma: Tribunal Europeo de Derechos Humanos. Obtenido de https://www.echr.coe.int/documents/convention_spa.pdf

Cooley, T. (1879). *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract .* Chicago: Callaghan and Company. Obtenido de https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books

Corte Constitucional del Ecuador. (2014). *Sentencia No. 001-14-PJO-CC.* Cuenca: Corte Constitucional del Ecuador. Obtenido de https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=001-14-PJO-CC

Corte Constitucional del Ecuador. (2020). *Sentencia No. 1868-13-EP/20 CASO No. 1868-13-EP.* Quito: Corte Constitucional del Ecuador. Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOicyNzE4ZjljZC1hZjU4LTQxMTItYjBkYi01MjVlYmUwNDU2ZjgucGRmJ30=

Defensoría del Pueblo. (2021). *Informe Anual sobre el cumplimiento del Derecho Humano de Acceso a la Información Pública Periodo de Enero a Diciembre de 2020.* Quito: Defensoría del Pueblo. Obtenido de https://www.dpe.gob.ec/wp-content/dpedocumentoslotaip/cumplimientolotaip/INFORME-LOTAIP-2020.pdf

Derechos Digitales; APC. (2020). *Requisitos mínimos para la Ley de Protección de Datos Personales de Ecuador.* Nueva York: APC. Obtenido de https://www.apc.org/es/pubs/requisitos-minimos-para-la-ley-de-proteccion-de-datos-personales-de-ecuador.

Díaz, V. (2021). Banco Pichincha confirma 'incidente de ciberseguridad' en sus sistemas. *El Comercio*, pág. Digital. Obtenido de https://www.elcomercio.com/actualidad/negocios/banco-pichincha-ciberseguridad-ciberataque-hackeo.html

Díaz, V. (2023). El Ministerio de Salud debe explicaciones sobre nueva filtración de datos personales. *La Barra Espaciadora*, pág. Digital. Obtenido de https://www.labarraespaciadora.com/ddhh/ministerio-de-salud-filtracion-de-datos-personales/

Dirección Nacional de Registro de Datos Públicos. (2015). *Norma de Asequibilidad a Datos Personales de los Registros Públicos.* Quito: Dirección Nacional de Registro de Datos Públicos. Obtenido de https://vlex.ec/vid/reformese-norma-regula-asequibilidad-638591061

El Telégrafo. (2019). Millones de datos de ecuatorianos se filtraron de servidor en Miami. *El Telégrafo*, pág. Digital. Obtenido de https://www.eltelegrafo.com.ec/noticias/tecnologia/1/datos-ecuatorianos-filtracion-servidor-miami

Enríquez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Revista de Derecho Foro, 1*(27), 43-61. Obtenido de https://revistas.uasb.edu.ec/index.php/foro/article/view/500

Enríquez, L. (2019). La Visión de América Latina sobre el Reglamento General de Protección de Datos. *Comentario Internacional, 1*(19), 99-112. doi:doi.org/10.32719/26312549.2019.19.4

Fernández, S., Pérez, J., & Galdámez, A. (2022). *Nuevos enfoques sobre transparencia y derecho de acceso a la información pública.* Pamplona: Editorial Aranzadi.

Fundamedios. (2021). Ministerio de Salud ratificó la filtración de datos y apunta a periodista y ciudadanos que dieron la alerta . *Fundamedios*, pág. Digital. Obtenido de https://www.fundamedios.org.ec/alertas/salud-ratifico-filtracion-datos/

Galvis, L. (2019). *Protección de datos personales de niños, niñas y adolescentes. En el marco de la juridificación y prevención del riesgo digital en Colombia.* Bogotá: Universidad Santo Tomás. Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/22124/2020%20lucero%20galvis.pdf?sequence=1&isAllowed=y

González, A. (2015). *Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva.* Toledo: Universidad de Castilla-La Mancha. Obtenido de https://dialnet.unirioja.es/servlet/tesis?codigo=80236

Guzmán, M. (2013). *El Derecho Fundamental A La Protección De Datos Personales En México: Análisis Desde La Influencia Del Ordenamiento Jurídico Español.* Madrid: Universidad Complutense de Madrid. Obtenido de https://docta.ucm.es/entities/publication/aaf99be2-a9d5-434c-bd82-6402df4aa665

Jehl, L., & Friel, A. (2018). *CCPA and GDPR Comparison Chart.* California. Obtenido de https://content.next.westlaw.com/w-016-7418?cid=9072277&chl=int&sfdccampaignid=7014O000001JkmVQAS&transitionType=Default&contextData=%28sc.Default%29

Kent, M. (2009). Property and Privacy: The Common Origins of Property Rights and Privacy Rights. *Campbell University School of Law , 2*(1), 1-22. Obtenido de https://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1077&context=fac_sw

(1948). *La Declaración Universal de los Derechos Humanos.* Paris: Asamblea General de las Naciones Unidas. Obtenido de https://www.un.org/es/about-us/universal-declaration-of-human-rights

(2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.* Quito: Congreso Nacional. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

(1998). *Ley de Protección de la Privacidad en Línes de los Niños.* Estados Unidos: Federal Trade Commission. Obtenido de https://www.ftc.gov/system/files/2012-31341.pdf

(1992). *Ley Especial de Telecomunicaciones.* Quito: Congreso Nacional. Obtenido de http://www.oas.org/juridico/PDFs/mesicic4_ecu_especial.pdf

(2021). *Ley Orgánica de Protección de Datos Personales.* Quito: Asamblea Nacional. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Montalbano, L. (2020). *El reglamento europeo de protección de datos personales y el derecho al olvido.* Madrid: Universidad Complutense de Madrid. Obtenido de https://eprints.ucm.es/id/eprint/59182/1/T41727.pdf

Murillo, P. (2010). La protección de los datos de carácter personal en el horizonte de 2010. *Anuario Facultad de Derecho-Universidad de Alcalá, 1*(2), 131-142. Obtenido de https://ebuah.uah.es/dspace/bitstream/handle/10017/6440/proteccion_murillo_AFDUA_2009.pdf?sequence=1&isAllowed=y

Palop, M. (2017). *Protección Jurídica de menores víctimas de violencia de género a tráves de Internet (Vulnerabilidad de la menor en sus relaciones de pareja, ciberacoso y derecho al olvido).* Castellón de la Plana: Universitat Jaume. Obtenido de https://www.tesisenred.net/bitstream/handle/10803/461919/2018_Tesis_Palop%20Bellosch_Melania.pdf?sequence=1&isAllowed=y

Parejo, L. (1993). El derecho fundamental a la intimidad. En M. Sauca, *Problemas actuales de los derechos fundamentales* (págs. 293--310). Madrid: Ius et Praxis.

Pfeffer, J. (2010). El juego del poder. *Harvard Business Review, 88*(6), 52-61. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3245444

Piñar, J. (2010). *¿Existe privacidad? en protección de datos personales, compendio de lecturas y legislación.* México D.F.: Tiro Corto Editores.

Roldán, F. (2021). Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review, 8*(1), 175-202. doi:10.18272/ulr.v8i1.2184

Saldaña, M. (2007). La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de información personal en los Estados Unidos. *Araucaria.*

Revista Iberoamericana de Filosofía, Política y Humanidades, 9(18), 85-115. Obtenido de https://www.redalyc.org/pdf/282/28291805.pdf

Serrano, R. (2022). *Datos personales en Ecuador: Análisis del Proyecto de Ley de Protección de Datos Personales.* Guayaquil: AMCHAM. Obtenido de https://amchamgye.ecuadesigners.com/corralrosales-datos-personales-en-el-ecuador-analisis-del-proyecto-de-ley-de-proteccion-de-datos-personales/

Tapia, E., Ruiz, R., & Vega, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Revista Misión Jurídica, 14*(20), 142-158. doi:doi.org/10.25058/1794600X.1912

Tribunal Constitucional del Ecuador. (2021). *Sentencia nº 2064-14-EP/21.* Quito: Tribunal Constitucional del Ecuador. Obtenido de https://www.informatica-juridica.com/sentencia/sentencia-del-tribunal-constitucional-del-ecuador-del-27-de-enero-de-2021-sentencia-no-2064-14-ep-21/

Unión Europea. (2000). *Carta de los Derechos Fundamentales.* Niza: Unión Europea. Obtenido de https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Vargas, J. (2013). *El Tribunal Constitucional y las garantías de derechos fundamentales: análisis general y procedimiento de: amparo, habeas data, habeas corpus, inconstitucionalidad.* Editorial Soto Castillo.