FACULTAD DE DERECHO Y CIENCIAS SOCIALES

“LA INADECUADA REGULACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO DEL ECUADOR.”

Autor

Jordan Xavier Borja Morales

Año
2019

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

“LA INADECUADA REGULACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO DEL ECUADOR.”

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesor Guía

Mgs. Rafael Eduardo Serrano Barona

Autor

Jordan Xavier Borja Morales

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo “La Inadecuada Regulación Para La Protección De Datos Personales En El Ordenamiento Jurídico Del Ecuador”, a través de reuniones periódicas con el estudiante Jordan Xavier Borja Morales en el semestre 201910, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación. “

_____

Rafael Eduardo Serrano Barona
Magíster en Derecho Energético y Recursos Naturales
C.C. 1712980935

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo “La inadecuada regulación para la protección de datos personales en el ordenamiento jurídico del Ecuador.” en el semestre 201910, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Lorena Naranjo Godoy
Magíster en Derecho de las Nuevas Tecnologías
C.C.170893780

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Yo, Jordan Xavier Borja Morales, declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

Jordan Xavier Borja Morales
C.C: 1719284620

AGRADECIMIENTOS

Gracias a todas las personas que fueron parte de este camino, a los que SIEMPRE han estado y estarán, a los que estuvieron desde el inicio y aún están aquí, los que se fueron sumando y también a los que se perdieron en el camino. Gracias a todos por ser parte de este camino.

DEDICATORIA

Para Lula, quien me enseño que en esta vida todos tienen sus “tiempos”, y a todos nos llega el momento.

RESUMEN

Este trabajo de investigación responde a la siguiente pregunta ¿es adecuada la regulación para la protección de datos personales en el Ecuador? Ante esta interrogante el primer y segundo capítulo se enfocó en definir e indicar de manera precisa en qué consiste los datos de carácter personal, el marco constitucional que lo cubre y su importancia jurídica, económica y social. En el tercer capítulo se realizó un análisis de la normativa existente en el Ecuador sobre datos personales, para lo cual se permitió hacer hincapié en la necesidad de contar con ley específica para su protección. Finalmente, en el cuarto capítulo se realizó un estudio acerca del desarrollo normativo internacional en materia de datos personales. De igual manera en este capítulo se analiza el contenido de normas internacionales representativas en materia de protección de datos y propone un contenido mínimo que deberá contener una ley de protección de datos personales en el Ecuador como solución a esta problemática jurídica.

ABSTRACT

This research work answers the following question: is the regulation for the protection of personal data in Ecuador inadequate? In response to this question, the first and second chapters focused on defining and indicating precisely what constitutes the personal data, the constitutional framework that covers it and its legal, economic and social importance. In the third chapter an analysis was made of the existing regulations in Ecuador on personal data, for which it was allowed to emphasize the need to have a specific law for their protection. Finally, in the fourth chapter a study was made about the international normative development in the field of personal data. Similarly, this chapter analyzes the content of representative international standards on data protection and proposes a minimum content that must be contained in a law on the protection of personal data in Ecuador as a solution to this legal problem.

ÌNDICE

INTRODUCCIÓN

La Constitución del Ecuador en su artículo 1, declara que el Ecuador es un Estado constitucional de derechos y justicia, colocando a los derechos tanto individuales como colectivos y de la naturaleza en una posición privilegiada. Es un alto deber del Estado ecuatoriano el garantizar sin discriminación alguna el efectivo goce de los derechos reconocidos en la Constitución. Por lo que resulta una grave afectación al ciudadano que, a pesar de que se encuentra enunciado en el artículo 66 numeral 19 el Derecho a la Protección de Datos de Carácter Personal, este no se encuentre correctamente desarrollado en el ordenamiento jurídico del país.

Los datos personales en la actualidad son considerados como “el nuevo petróleo”, un preciado combustible sin el cual no es posible hacer funcionar la maquinaria de muchos de los negocios de hoy en día. (Morell, 2014). Esta libre circulación de datos personales beneficia el desarrollo económico, pero puede venir atado a la lesión de los derechos de las personas, en especial la intimidad, ya que en su contenido encontramos elementos que pueden describir a una persona, sus hábitos y su pensamiento.

Ante el inmenso mercado de los datos personales y su posible afectación al ciudadano, considerando que su protección es un derecho, se vuelve obligatorio el preguntarse ¿es adecuada la regulación para la protección de datos personales en el Ecuador?

Para contestar esta interrogante es necesario hacer una conceptualización de datos personales y de los derechos que se encuentra involucrados en su tratamiento. Debemos revisar el desarrollo normativo internacional en el cual se consagran principios para el tratamiento de datos, facultades de los titulares de los datos y demás componentes que generan un estándar de protección de datos personales para así poder compararlo con la regulación existente en el ordenamiento jurídico ecuatoriano.

Vamos a concluir que Ecuador necesita adoptar una ley de protección de datos personales que proteja y desarrolle el derecho constitucional reconocido. Esta ley debe seguir los estándares internacionales o los lineamientos establecidos en las normas de los países vecinos y las que tengan directa influencia en el país. Al seguir estos lineamientos podremos estar en posición similar en el tratamiento de datos personales, los que nos permitirá competir en el mercado internacional.

1. DEFINICIÓN DE DATOS PERSONALES Y SU IMPORTANCIA.

En el presente capitulo definiremos que son los datos personales desde la doctrina y el desarrollo normativo. Su importancia y relevancia jurídica, económica y social.

1.1 Importancia de los Datos Personales

La época actual se conoce como la sociedad de la información, se caracteriza por el gran avance de las tecnologías tanto de la información como de las telecomunicaciones.

La sociedad de la información promueve la sociedad del conocimiento, la Unesco la define como la sociedad inspirada en el saber (Ministerio de Telecomunicaciones y Sociedad de la Infomración [MINTEL], 2018, p. 10).
El avance de las tecnologías ha logrado brindar nuevas formas de relacionarse con el mundo. Las personas tienen a la mano la posibilidad de informarse o comunicarse a una gran velocidad.

El desarrollo de las nuevas tecnologías se centra en el uso del internet, la red de redes que permite conectar millones de usuarios. (Conde, 2005, p.15). La red es esencialmente de uso libre, fuera del control de cualquier país y regulación. Por lo tanto, se hace indispensable que el ordenamiento jurídico se acomode con el fin de dar solución a los problemas que pueda causar el uso sin control del internet.

Sobre la importancia económica de los datos de carácter personal la Autora Concepción Conde Ortiz menciona:

> Se ha observado que mientras la sociedad industrial tuvo como objetivo la producción de bienes materiales, la sociedad post industrial se basa en la producción y transmisión de informaciones. A la sociedad de la información la definen los bancos de datos y las redes de información" (Conde, 2005, p.16).

Los datos personales en la actualidad son utilizados por la mayoría de las empresas, y también por los Estados para el desarrollo de sus actividades y funciones.

Es importante anotar que, para el cumplimiento de los fines de un Estado, es necesario se cuente con determinada información de los ciudadanos, del mismo modo que un uso no regulado de esa información puede distorsionar gravemente el funcionamiento social (Rebollo y Serrano, 2017, p. 33).

Los datos personales son de gran utilidad para el sector público y privado. El sector privado requiere o puede utilizar los datos personales para determinar los sectores de mercado para la venta de productos, clasificar a las personas como potenciales clientes en función de sus hábitos de consumo, marcas predilectas o capacidad económica, y comercialización de servicios e impacto en el mercado. El sector público debe utilizar los datos de las personas exclusivamente para cumplir sus funciones. Para elaborar sus políticas públicas requieren administrar y procesar datos respecto a antecedentes personales o nominaríamos. El Estado necesita datos para tomar decisiones racionales y evaluar el impacto de su gestión, "por ejemplo, que el Estado pueda conocer sus rentas y su situación familiar para asignar un subsidio, pensiones o beneficios de educación, sus datos de salud para fijar políticas asistenciales, su domicilio para el padrón electoral" (Jijema Leiva, 2013, p. 52). Por lo tanto, el Estado tiene la obligación legal de tratar datos personales de los ciudadanos.

Por otro lado, además de la cantidad de datos con lo que cuentan el sector privado y los Estados, también hay que precisar la procedencia de los mismos. La mayoría son generados por las mismas personas mediante el uso de sistemas informáticos o diferentes servicios de red como email, redes sociales, motores de búsqueda, teléfonos inteligentes, etc. No obstante, no todos los datos personales provienen del uso de la red, sino que en tareas cotidianas como abrir una cuenta de ahorros, llenar un formulario para el ingreso a una universidad, todo esto es la entrega de datos de carácter personal.

La tecnología actual facilita el manejo de información en gran escala y con gran velocidad y eficiencia. Muchos de los datos recopilados son datos personales, los cuales pueden dar una descripción de una persona, de sus características físicas, sociales, económicas, sociales, etc. Componentes de la esfera más íntima de las personas. La utilización discrecional y el tratamiento de datos en manos de terceros es un riesgo que puede llegar a afectar los derechos y las libertades fundamentales.

Por la gran importancia que han obtenido los datos personales, es necesario que se regule mediante la norma el uso que se hace de los mismos, puesto que es de vital importancia que estos datos no circulen de forma libre, sin ningún tipo de control o vigilancia, además que todo tratamiento se realice desde un punto de vista legal y legítimo. Con el fin de precautelar la integridad e inviolabilidad de los derechos consagrados de las personas.

1.2 ¿Qué son datos personales?

La mayoría de legislaciones y autores en el mundo nos brindan una definición similar de lo que son los datos personales, en primer lugar tomaremos la definición que nos brinda el artículo 2 del Convenio Nro. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual menciona que “Datos de carácter personal significa cualquier información relativa a una persona física identificada o identificable.”

En el ordenamiento jurídico español la recién derogada Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal toma la definición del convenio 108, en su artículo 3: “cualquier información concerniente a personas físicas identificables o identificadas. Del mismo modo en Colombia la Ley 1581 de 2012 para El Tratamiento de datos también adopta esta definición en su artículo 3 numeral c: “Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”.

Por su parte la Ley general de protección de datos personales en posesión de sujetos obligados (México) de 26 de enero de 2017, en su artículo 3 define datos personales: como cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

La definición presentada por el convenio 108 guarda armonía y la vez es ampliado por el artículo 3 del Reglamento Europeo (UE) 2016/679 del PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril 2016, relativo a la protección de las personas físicas en lo que respecta el tratamiento de datos personales y a la libre circulación de estos datos (GDPR por sus siglas en ingles), el cual menciona:

> «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

Esta definición toma su base en la definición contenida en la Directiva 95/46/Ce del Parlamento Europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. En esta definición podemos destacar las siguientes componentes “toda información”, “persona física”, “identificada o identificable”. “identificador”.

En el Ecuador encontramos una escueta definición de datos personales que se encuentra en la disposición general novena de la Ley de comercio electrónico, firmas y mensajes de datos la cual menciona que datos personales: “son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley”. Esta definición confunde e integra en la misma categoría tanto datos personales, como datos íntimos. Por lo tanto, es imprecisa y no tiene concordancia con la definición usada en el derecho comparado. Una nueva definición la encontramos en el Reglamento a Ley orgánica de gestión de la identidad y datos civiles en el artículo 2 numeral 5 son datos personales: “aquellos que permiten identificar o volver identificable a una persona natural” la cual guarda cierta concordancia con la definición contenida en el convenio 108 de la unión europea.

Un elemento en común de la mayoría de legislación concerniente a la protección de datos es que han excluido en su ámbito de aplicación a las personas jurídicas. “La protección de esas personas se encuadra mejor en el derecho de sociedades, propiedad intelectual, defesa de la competencia y en otras varias no incluyendo bajo el concepto de datos personales e intimidad” (Davara , 2001, pp. 83-85). Sin embargo, la Ley de protección de datos personales uruguaya del año 2008, define los datos de carácter personal como “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables” y menciona en el ámbito subjetivo “que el derecho a la protección de datos personales se aplicara por extensión a las personas jurídicas, en cuanto corresponda”.

Los datos personales son en principio inherentes únicamente a personas naturales. Sin embargo, “los datos referidos a ciertos sujetos de hecho

(sociedad sin personalidad jurídica o un grupo no familiar), podrían dar a conocer datos concernientes a personas físicas con lo que se podría directamente afectar su intimidad". (Grimalt, 1999, pp.56-58). En otras palabras, si los datos de una persona jurídica o sujetos de hecho pudieren atribuirse a una persona física la cual pueda ser identificable, podrán ser entendidos como datos personales.

La definición de datos personales hace referencia a datos atribuibles a una persona, que la identifiquen, que puedan facilitar la configuración de un perfil, aunque no pertenezcan al reducto de la intimidad de la persona. (Troncoso, 2010, p.133)

El concepto de datos personales no separa a ningún tipo de información por intrascendente o insignificante que pudiera parecer. El dato personal es cualquier tipo de información sea está numérica, alfabética, gráfica, fotográfica, fonográfica, acústica o de cualquier otro tipo referida a la persona de que se trate. Es indiferente que dicha información pueda ser subsumida o no dentro del grupo de datos que *per sé* pertenecen a la esfera protegida por la intimidad a los efectos de delimitar el concepto de dato personal (Grimalt, 1999, p. 45).
Los datos personales se consideran como tal cuando pueden describir a la persona o brindar un perfil de ella por ejemplo en cuanto le dan identidad, la describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. "Los datos que son de conocimiento público no dejan, por ello, de pertenecer al poder de disposición de la persona" (Troncoso, 2010, p. 133) "También pueden describir aspectos más sensibles como su forma de pensar, estado de salud, características físicas, ideología o vida sexual entre otros." (Negro Alvarado, 2014). Estos últimos se los conoce como datos personales sensibles.

En conclusión, los datos personales son toda tipo de información sea numérica, alfabética, gráfica, fotográfica, fonográfica, acústica o de cualquier otro tipo, que pueda ser atribuida a una persona natural, es decir a cualquier miembro de

la especie humana, mediante la cual se puede identificarle, aunque esta información sea intranscendente o insignificante. Los datos personales pueden brindar una descripción de la persona, en cuanto le dan identidad, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional, o recojan información biométrica, genética y relativa a la salud. Del mismo modo pueden describir aspectos más sensibles de la persona sea este su pensamiento, vida sexual, origen étnico, etc.

1.3 Datos Personales sensibles o especialmente protegidos.

En todo uso de información de carácter personal puede afectar los aspectos vulnerables de las personas. Adicional al peligro que incorpora el tratamiento de datos personales, existen datos específicos que por sí mismo representan un peligro innato de afectar aspectos especialmente sensibles.

La Declaración de Madrid sobre Estándares Internacionales sobre Protección de Datos personales y privacidad del 5 de noviembre de 2009 (Resolución de Madrid), define a los datos sensibles como “la información de carácter personal que afectan a la esfera más íntima del interesado o cuya indebida utilización pueda originar discriminación”. Los Estándares de Protección de Datos Personales, expedido por la Red Iberoamericana de Protección de Datos de 20 de junio de 2017, define a los datos personales sensibles como:

> Aquellos que se refieren a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico: creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Materialmente los datos sensibles son aquellos que hacen referencia a cualidades de las personas relacionadas con su dignidad, son aspectos que afectan a su personalidad, que dibujan su forma de ser o de comportarte (Rebollo y Serrano, 2017, p.245).

Particularmente se considera sensible aquellos datos que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como datos relativos a la salud o a la sexualidad, la afiliación sindical, entre otras. “Son datos que por tener directa transcendencia sobre la intimidad de las personas merecen una protección más reforzada, y su tratamiento puede acarrear que sean conocidos por terceros a los que no queremos hacer partícipes” (Conde, 2005, p. 69).

El concepto de datos personales sensibles incluye los datos biométricos, genéticos y relativos a la salud. El GDPR en su artículo 9 los categoriza como una categoría especial de datos personales que merecen mayor protección.

La normativa europea GDPR en su artículo 2 define a los datos biométricos como: “datos personales obtenidos a partir de un tratamiento técnico específico, relativos a características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identidad única de dicha persona, como imágenes faciales o datos dactiloscópicos”. Los datos biométricos más utilizados son la huella dactilar, el iris del ojo, la palma de la mano y los rasgos del rostro. Los datos biométricos en la actualidad se utilizan en temas relacionados a seguridad. Reglamento del Mintel 009-2017, de política pública para fortalecer la identificación, registro de datos civiles y prestación de servicios electrónicos, en el marco de la sociedad de la información, define los datos biométricos como “los datos obtenidos a partir de un proceso biométrico. Comprende observaciones preliminares, muestras biométricas, modelos, plantillas y valoración o comparaciones.

El dato genético lo define en el mismo artículo 2 del GDPR como: “datos personales relativos a las características genéticas heredadas o adquiridos de

una persona física que proporcionen una información única sobre la fisiológica o la salud de esa persona, obtenidos en partículas del análisis de una muestra biológica de tal persona".

La Constitución de la República del Ecuador en su artículo 92 declara que para la recopilación de datos sensibles cuando exista necesidad será necesario contar con la autorización expresa de la ley o de la persona titular, se exigirá también la adopción de medidas de seguridad.

1.4 Datos Personales que por disposición de la ley deben constar en registros públicos y por ello son accesibles al público.

Los Estados para el cumplimiento de sus actividades tienen la necesidad de llevar un registro de identificación de todos los ciudadanos, por lo tanto, realiza un tratamiento de datos personales sin necesidad de contar con la autorización de los ciudadanos titulares de los datos, esto quiere decir que recopila datos por mandato de la ley.

El hecho que la ley otorga la categoría de datos públicos a determinada información no le quita la característica de datos personal, por lo tanto, se mantiene la titularidad sobre los mismos por parte de las personas

2. DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales es un derecho, el cual se encuentra garantizado en la Constitución. El tratamiento y uso de datos personales puede causar un daño a otros derechos fundamentales. El derecho a la protección de datos personales es una evolución normativa, tiene su origen en la intimidad, del que se separa gradualmente hasta que se reconoce su autonomía a través de la jurisprudencia y de la normativa constitucional (Naranjo Godoy , 2018, p. 65)

2.1 Derecho a la Intimidad

El derecho a la intimidad ha evolucionado, desde un derecho a la defensa o a la no intromisión, hasta convertirse en un derecho que posibilita a las personas el control de las cosas que son inherentes a su esfera más cerrada, la capacidad de decir sobre si desea exteriorizarlos o prohibir la intromisión de terceros.

El artículo 12 de la Declaración Universal de los Derechos Humanos proclamado por la asamblea general de la ONU, determina que:

> "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Por su parte, en la misma línea, el Pacto Internacional de Derecho Civiles y Políticos (16 de diciembre de 1966) en su artículo 17 señala que "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". Del mismo modo, la Convención Americana sobre Derechos Humanos en su artículo 11, apartado segundo establece que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales en su honra o reputación".

El derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer, sea a particulares o poderes públicos, su voluntad de no dar a conocer dicha información (Conde, 2005, p. 23). Esto lo constituye en un pilar fundamental para justificar la protección de datos personales y la necesidad de contar en el ordenamiento jurídico herramientas que cumplan este fin. El hombre tiene

derecho a que los demás no se entrometan en su vida privada, así como necesita de la comunicación, necesita también soledad, para desarrollar sus virtudes y asumir errores. (Uicich, 1999, p.31)

El diccionario de la Real Academia de la Lengua define a la intimidad como “zona espiritual reservada o intima de una persona o de un grupo, especialmente de una familia” (Real Academia Española, 2017). “La intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más internas, como la ideología, religión o creencias, tendencias respecto a la sexualidad, problemas de salud que deseamos mantener en secreto u otras inclinaciones” (Conde, 2005, p. 25)

Es necesario diferenciar a la intimidad de la privacidad, la cual hace referencia al ámbito personal formado por su vida familiar, aficiones, bienes particulares y actividades personales. Los cual constituye también una esfera que se debe proteger.

La teoría de las esferas alemanas o círculos concéntricos explique que el núcleo o lo más interior constituye lo íntimo, en una parte más externa encontramos lo familiar, en otra lo secreto o confidencial, y siendo la última esfera lo público. “Estas esferas no son uniformes, sino que cada individuo las configura atendiendo a sus pretensiones de forma completamente libre (Rebollo y Serrano, 2017, p.34). En contra de la teoría de las esferas Madrid Concesa ha formulado la teoría del mosaico quien explica que

> La teoría de las esferas no es válida, dado que hoy los conceptos de lo público y lo privado son relativos, pues existen datos que a priori son irrelevantes desde el punto de visa del derecho a la intimidad, pero que unidos pueden configurar una idea completa de cualquier individuo, al igual que pequeñas piedras que componen un mosaico” (Rebollo y Serrano, 2017, pp. 35-36)

En el uso de las tecnologías y el manejo de datos de carácter personal, uno de los bienes jurídicos más propensos a ser lesionados es el de la intimidad. La Constitución de la República del Ecuador en su artículo 66 numeral 20 declara: “se reconoce y garantizará a las personas, el derecho a la intimidad personal y familiar”.

2.2 Derecho a guardar reserva sobre las convicciones.

Adicional al derecho autónomo a la protección de datos personales la Constitución de la República del Ecuador reconoce que ninguna persona podrá ser obligada a revelar ante nadie los componentes de su esfera más íntima, La Constitución de la República del Ecuador en su artículo 66 numeral 11, garantiza a las personas:

> “el derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica”.

No existe en el Ecuador un desarrollo con respecto a los contenidos de este derecho, pero podemos deducir que la protección respecto a los pensamientos tiene un vínculo directo tanto con la intimidad, como al derecho autónomo a la protección de datos personales.

El artículo 7 de la Ley orgánica de protección de datos personales española, menciona en concordancia con la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Estos datos para lo cual se podrá guardar reserva, cumplen con las características de ser datos sensibles, por lo que su tratamiento puede generar discriminación

2.3 Derecho Autónomo a la Protección de Datos Personales.

El derecho te protección de datos personales entendida como la protección jurídica en lo que concierne al tratamiento de sus datos de carácter personal. (Conde, 2005, p.29). Les otorga a las personas facultades jurídicas como el poder de decidir en lo concerniente al tratamiento de los datos de carácter personal. En especial cuando sea objeto de tratamiento, levantamiento, almacenamiento o comercialización de los mismos por parte de terceros personas no autorizadas.

Al derecho de protección de datos se le nombra tanto en la legislación como en la doctrina de diferentes maneras: para la doctrina alemana se lo conoce como autodeterminación informativa, refrendada por la sentencia de 15 de diciembre de 1983 del Tribunal Constitucional alemán:

> La facultad del individuo, deriva de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la vida propia" entendiendo el derecho a la autodeterminación informativa como la facultad general de disponer de los datos propios. (Domínguez, 2016, p. 93)

Del mismo modo se han utilizado los términos intimidad informática que hace mención de las garantías que facilitan el control de los datos personales y libertad informativa. Los cuales no agotan los contenidos respecto a la protección de datos personales, ya que tratan respecto a la capacidad de decidir si los datos pueden ser objetos de tratamiento.

Creemos que lo más adecuado es denominarlo derecho a la protección de datos personales, ya que esta denominación es más amplia, sus contenidos versan respecto a la titularidad de los datos personales y el poder de decidir sobre ellos. También incluye la facultad de los titulares al acceso, rectificación, cancelación y oposición como derechos de los titulares. No limita a la utilización

de medios tecnológico, sino que protege de cualquier tipo de injerencia sobre los datos personales. El objeto de protección del derecho a la protección de datos personales es cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar sus derechos. (Troncoso, 2010, p. 133)

El derecho a la protección de datos personales es la evolución normativa, extiende las garantías del derecho a la intimidad y abarca los bienes de la personalidad que se refieren a la vida privada vinculada a cualquier dato personal. Es así que el derecho a la protección de datos personales se deriva del derecho a la privacidad (Villalba, 2018, p. 36).

Es necesario diferenciar el derecho autónomo a la protección de datos personales con el derecho a la intimidad. El primer punto de diferencia es el objetivo de cada derecho. “El derecho a la intimidad protege los datos íntimos, por el hecho de serlo, deben estar excluidos del conocimiento de los demás; en cambio, el derecho a la protección de datos tutela cualquier dato, sea o no íntimo” (Troncoso, 2010, p. 133). Por consiguiente, es un derecho que da una protección más amplia que el derecho a la intimidad.

La segunda diferencia es que el derecho a la intimidad es un derecho que exige la no intervención de poderes públicos y de particulares en la esfera íntima de las personas. Por su parte, el derecho autónomo a la protección de datos de carácter personal atribuye a las personas facultades positivas para controlar la información personal. La disposición y el control sobre los datos personales se proyectan en un conjunto de principios y derechos que configuran el contenido del derecho a la protección de datos personales. (Troncoso, 2010, pp. 134-136)

La Constitución de la República del Ecuador, en su artículo 66 numeral 19 declara:

> Se reconoce y garantizara a las personas el derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información, requerirán la autorización del titular o el mandato de la ley.

Como nombra la Constitución se garantiza la necesidad de brindar la autorización de la persona titular para legitimar el tratamiento de datos de carácter personal. El Tribunal Constitucional español en sentencia 292/2000, con respecto a la protección de datos personales señala:

> "el reconocimiento del derecho a ser informado de quien posee sus datos y con qué fin, y el derecho a oponerse a esa posesión o uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de datos".

El primer aspecto fundamental del contenido del derecho a la protección de datos personales es el poder de decir sobre ellos. Siempre el tratamiento de datos debe estar amparado en la prestación informada del consentimiento para su legitimación. En consecuencia, este aspecto supone que el titular de los datos es el único que tiene derecho a decidir quién, cómo, cuándo y para qué se tratan sus datos (Augusto Orrero, 2013, p. 326).

El GDPR en su artículo 4 numeral 11 define el consentimiento del interesado como "toda manifestación de voluntad libre específica, informada e inequívoca por la que le interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". "la manifestación de voluntad es una forma de proyectar al exterior lo que pensamos o decidimos por medio de una acción o de una omisión, por lo que se puede aceptar en la protección de datos el consentimiento tácito" (Rebollo y Serrano, 2017, p. 119)

El segundo aspecto fundamental del contenido del Derecho a la Protección de datos personales es un conjunto de derechos que garantizan la protección, es decir los derechos que garantizan la eficacia del consentimiento y del control en el ámbito del tratamiento (Rebollo y Serrano, 2017, p. 181). Este conjunto de derechos los podemos nombrar como derecho ARCO y están formados por el derecho de acceso, rectificación, cancelación y oposición.

El derecho al acceso es la posibilidad de comprobar si se dispone de información sobre uno mismo y conocer el origen del que procede la existente y la finalidad con que se conserva (Murillo y Piñar, 2009, p. 187) el acceso engloba la facultad de conocimiento de la información contenida, su origen y finalidad, y al mismo tiempo, su comunicación. La titularidad del derecho al acceso permite solicitar la búsqueda dentro de bases de información de los datos de la persona y se entenderá por cumplida cuando se ponga a su disposición la información solicitada.

La finalidad de la rectificación es que los datos sean correctos. La rectificación puede ser requerida cuando los datos contenidos sean incorrectos, imprecisos, o este desactualizados. El derecho a la rectificación y el derecho a la cancelación según la sentencia del Tribunal Constitucional Español 292/2000, forman parte del contenido esencial del derecho a la protección de datos y vienen a hacer efectivo, en el supuesto de datos inexactos o incompletos (Rebollo & Serrano, 2017, p. 201).

El derecho a la cancelación la cual persigue la supresión de los datos que resulten inadecuados o excesivos, o porque ya no resulte necesario para el fin de las actividades. Es el derecho del titular a que se excluyan del tratamiento datos de carácter personal, ya sea por ser erróneos, o por no interesarle que se sometan a tratamiento (Aparicio, 2000, p. 139).

La cancelación, no origina en un primer momento la desaparición del dato, sino en muchas ocasiones el bloqueo de los mismos, que constituye el paso previo

a la supresión definitiva posterior. (Rebollo y Serrano, 2017, pp. 202-203). Con respecto a la relación entre el habeas data y derecho de cancelación el autor Omar Frutos Mendoza menciona:

> “El derecho de cancelación también es conocido en el ámbito iberoamericano con los nombres “Habeas Data Cancelatorio y Habeas Data de Exclusión”, coinciden en que el derecho consiste en la facultad que tiene el titular de los datos de carácter personal para solicitar la eliminación de su información.” (Frutos Mendoza, 2013, p. 15).

odemos definir el derecho de oposición como el derecho de titular de los datos personales a negarse, por motivos legítimos, a que sus datos personales sean objeto de tratamiento. Contempla la posibilidad de oponerse al tratamiento de los datos de carácter personal, en los casos que no sea preciso consentimiento y siempre que una ley no disponga lo contrario (Rebollo y Serrano, 2017, p. 207). El reglamento de desarrollo de la Ley orgánica de protección de datos española 15/1999 (RLOPD) en su artículo 34 define el derecho de oposición como “el derecho del afectado a que no se lleve a cabo un tratamiento de sus datos de carácter personal o se sede en el mismo”.

.

2.4 Nuevos Derechos

Con la entrada en vigencia del Reglamento de la Unión Europea 2016/679 respecto a la protección de datos personales de las personas naturales, se reconocieron una nueva ola de derechos. Estos derechos optimizan la capacidad de decisión y control sobre los datos personales. Estudiaremos dos de estos nuevos derechos reconocidos.

2.4.1 Derecho al Olvido.

Las sentencias 545/2015 de la sala civil del Tribunal Supremo español establecen que la información personal de una persona “va perdiendo su

justificación a medida que trascurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esa persona, carecen de interés histórico".

El derecho al olvido es la facultad que tienen las personas sobre sus datos personales para borrarlos, bloquearlos y suprimirlos "cuando contengan información personal que se considere obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de los derechos fundamentales". (Fernández, 2015, p. 225). Por lo tanto, es la garantía de las personas para que sus datos no circulen indefinidamente en la red, con el fin de salvaguardar la intimidad de la persona, la dignidad y el derecho a un buen nombre.

Por la variedad de información relativa a una persona que pudiese existir deberá proceder un análisis de cada caso. No es lo mismo que una persona requiera que no sean tratados datos personales utilizados en una red social, de la cual ya no quiere ser parte. Que aquella persona que requiera sea borrada el registro de una condena por una actividad delictiva, aunque ya la condena haya sido pagada. En el primer caso es razonable la petición de borrar los datos de la red, pero en el segundo estaría siendo contraria al interés público ya que la comisión de un delito no puede desaparecer de los registros (Rebollo y Serrano, 2017, pp. 296-287).

Respecto al derecho al olvido el GDPR en el artículo 17 reconoce el derecho del interesado a "obtener sin dilatación indebida del responsable del tratamiento la supresión de los datos personales inexactos que le conciernen. El cual estará obligado a suprimir sin dilatación alguna cuando concurra una de las circunstancias señaladas"

En el ámbito latinoamericano encontramos el derecho al olvido plasmado ley de Costa Rica en el artículo 10 del decreto 3755 de 2012, reglamento de la ley costarricense de protección de datos y en la ley de Nicaragua 787 de 2012 de protección de datos en su artículo 10.

2.4.2 Portabilidad de Datos personales

El GDPR reconoce a las personas titulares de los datos personales subidos a determinados servicios de internet, no solo cuentan con el derecho de corregirlos, retirarlos o eliminarlos. También tienen derecho a llevárselos o replicarlos en forma compatible con otras plataformas. “El control también significa poder mover sus datos de un lugar a otro, y tenerlos correctamente eliminados de la primera ubicación en el proceso”. (Puccinelli, 2017, p. 210)

El derecho a la portabilidad es un derecho autónomo que se relaciona directamente con el derecho al acceso, su objeto es darla al titular del derecho la posibilidad de cambiar entre diferentes proveedores de servicios. Solo se reconoce un derecho de portabilidad de datos a los que hayan sido otorgados con el consentimiento del titular, o derive de un contrato. Pero no incluyen los datos que genera el responsable del tratamiento. (Puccinelli, 2017, pp. 222)

La portabilidad de datos a vista del GDPR en su artículo 20 incluye los derechos a que se trasmitan los datos personales de un responsable a otro sin impedimentos, y a recibir del responsable del tratamiento los datos personales requeridos de manera gratuita, sin dilataciones y en formato estandarizado en lenguaje de uso común.

En el ámbito latinoamericano encontramos mención al derecho a la portabilidad en: la Ley general de protección de datos personales en posesión de sujetos obligados de México en su artículo 57, en la Ley Nro. 13.709 de Brasil sobre la protección de datos personales en su artículo 18 numeral V. También se hace mención al derecho a la portabilidad de datos personales en el Proyecto de ley de 15 de marzo de 2015 de Chile para regular la protección y el tratamiento de datos personales en su artículo 19, y en Proyecto de ley 147/2018 para la protección de datos personales argentino en su artículo 33.

3. ANÁLISIS DE LA REGULACIÓN JURÍDICA ECUATORIANA SOBRE DATOS PERSONALES

En el ordenamiento jurídico del Ecuador no existe una ley específica que regule la protección de datos personales. A pesar de no contar con un cuerpo normativo que regule esta materia, si existe regulación al respecto. Desde el reconocimiento constitucional como un derecho autónomo, hasta lineamiento para garantizar la protección en el tratamiento en manos de terceros. La regulación respecto a la protección de datos personales en el Ecuador se encuentra dispersa en diferentes cuerpos normativos y es imprecisa ya que no llega a tratar todos los contenidos de este derecho. Por lo tanto, vamos a realizar un análisis de toda la normativa actual existente en materia de datos personales, su protección y su tratamiento.

3.1 Constitución de la República del Ecuador

La Constitución es la norma suprema del Ecuador, en ella está contenido los derechos y garantías que tienen todos los ecuatorianos. El artículo 66 enumera el grupo de derechos denominado como derechos de libertad, en su numeral 19, reconoce el derecho a la protección de datos personales. Dentro de esta facultad se incluye los derechos al acceso y la decisión. Se garantiza a las personas la protección de datos de carácter personal y la necesidad de contar con la autorización del titular de los mismos o el mandado de la ley para la recolección, archivo, procesamiento, distribución o difusión.

La sola enunciación del derecho a la protección datos personales es insuficiente ya que por sí sola la Constitución no puede materializar el ejercicio del mismo. La limitación que cuenta es la falta de una definición exacta de que son datos de carácter personal. Tampoco la Constitución especifica si la protección de datos personales es solo para personas físicas, considerando que el artículo 10 de la constitución reconoce la titularidad de los derechos consagrados en la propia constitución y los instrumentos internacionales a

todas las personas sin discriminación. Reconociendo que tanto personas natural y jurídica son titulares de los derechos en los casos que apliquen.
En la Constitución no se nombra quien es la autoridad competente encargada de supervisar el cumplimiento de las normas jurídicas sobre protección de datos personales. Del mismo modo no establece mayor regulación respecto al manejo de datos por parte de instituciones públicas y privadas.

Es necesario destacar que, en la Constitución por sus propias características, no puede ni debe agotar todos estos temas, es necesario de que en el ordenamiento jurídico existan leyes que viabilicen, complementen, aumenten y garanticen los contenidos constitucionales.

3.2 Ley de comercio electrónico, firmas y mensajes de datos

La ley de comercio electrónico, firmas y mensaje de datos, entro en el año 2002, entre sus objetivos se encuentra regular además de los mensajes de datos y las firmas electrónicas, artículo 1 “la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información… y la protección de los usuarios de estos sistemas”.

Esta ley contiene una definición de datos personales que existe dentro del ordenamiento jurídico ecuatoriano, específicamente la encontramos en la disposición general número novena, la cual declara que datos personales: “son aquellos datos o información de carácter personal o íntimo”. El cual no define de manera precisa e inequívoca a los datos personales, además confunde en la misma categoría a los datos personales y los datos íntimos.

Dentro del articulado se hace mención del derecho de los titulares de los datos personales de expresar su consentimiento, para la elaboración de bases de datos, trasferencia o utilización de las mismas. El artículo 9 no especifica las formas y medios en los que deberá manifestarse este conocimiento. No regula el derecho al acceso, rectificación, oposición y cancelación, por lo tanto,

nuevamente nos encontramos ante una normativa imprecisa e incompleta, que no garantiza la protección de los datos personales en el Ecuador.

3.3 Ley orgánica de Telecomunicaciones.

La ley orgánica de telecomunicaciones, entro vigencia el 28 de febrero del año 2015, con el objetivo de desarrollar el régimen general de telecomunicaciones y espectro radioeléctrico como sectores estratégicos del Estado. Esta ley es aplicable a las personas naturales y jurídicas que realicen actividades relacionadas con telecomunicaciones, para garantizar el derecho y el cumplimiento de las obligaciones de los prestadores de servicios y los usuarios. Respecto a la protección de los usuarios o abonadas de sistemas de telecomunicaciones, se reconoce en el artículo 22 numeral 4 el derecho a la privacidad y a la protección de datos personales, por parte del prestador con el que contrate los servicios. En el reglamento general a ley orgánica de telecomunicaciones en su artículo 3 numeral 4 define a los prestadores de servicios de telecomunicaciones como “la persona natural o jurídica que posee el título habilitante para la prestación de servicios de telecomunicaciones, radiodifusión de señal abierta o por suscripción”. Por lo tanto, en concordancia con el articulo 24 numeral 14 estos son los obligados a adoptar las medidas necesarias para la protección de datos personales de los abonados.

La Ley de telecomunicaciones desarrollo al derecho a la intimidad consagrado en el artículo 66 numeral 20 de la Constitución del Ecuador, el cual de manera equivoca se busca garantizar con la protección de datos personales. Como ya lo hemos mencionado la protección de datos personales es un derecho autónomo reconocido en la Constitución, cuyos contenidos versan sobre el poder de los titulares de decidir sobre sus datos personales.

El derecho a la privacidad de los abonados se protege con las obligaciones de los prestadores de servicios de garantizar la no destrucción, perdida, alteración, revelación o acceso de terceras personas sobre los datos almacenados,

trasmitidos o tratados en la prestación de los servicios de telecomunicaciones. Por lo tanto, no se reconoce en el marco de esta ley los derechos ARCO a los abonados de servicios de telecomunicaciones, ni la capacidad supresión de los datos en el caso de que se dé por terminado le relación contractual.

Es importante destacar que ni la Ley telecomunicaciones ni su reglamento cuentan con una definición de datos personales. No menciona un régimen de responsabilidades ante la inadecuada protección de datos personales. Señala a Arcotel como la institución encargada de reglamentar y establecer los mecanismos para supervisar el cumplimiento de las obligaciones establecidas. Pero hasta la fecha no se ha expedido una resolución por parte de Arcotel que contenga los mecanismos de control o sanción en caso de violación de la protección de datos.

3.4 Código orgánico de la economía social de los conocimientos.

El régimen de propiedad intelectual en el Ecuador se encuentra regulado en el Código orgánico de la economía social de los conocimientos (COESC). Si bien no es materia de este código regular el derecho a la protección de datos personales, si se hace referencia dentro del mismo sobre el levantamiento y conservación de datos de carácter personal.

Se reconoce la protección de derechos de autor de las bases de datos que por razones de originalidad de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual. Pero especifica que la protección no se extenderá a los datos personales que pudiera contener las bases de datos protegidas. Los datos personales no podrán ser utilizados salvo que se cuente con autorización expresa del titular, mandato de la ley o por orden de autoridad judicial competente para ello o cuando las instituciones de derecho público lo requieran para el ejercicio de sus respectivas competencias.
La disposición general vigésima sexta del COESC, señala la obligación de las entidades públicas, personas naturales y personas jurídicas de derecho privado

que tengan en su poder archivos de datos personales, de contar con un portal o página web donde se informe a los usuarios respecto a los derechos que le asisten respecto a la protección de datos personales, incluido el uso, origen, destino y tiempo de vigencia de los banco de datos y los derechos a rectificación, eliminación de sus datos personales. Además, es obligación detallar las políticas y procedimientos para la protección de datos personales y servicios en línea para consultas y reclamos.

A pesar de contener un mandamiento legal de informar la posesión de datos personales y los derechos que goza el titular, no basta con su sola enunciación. El COESC no señala quien será la autoridad competente de vigilar y sancionar en caso de incumplimiento. Se puedo apreciar que actualmente esta normativa en su mayoría no se cumple, por lo tanto, no se garantiza el derecho a la protección de datos personales.

3.5 Código orgánico monetario y financiero

El Código orgánico monetario y financiero entro en vigencia el 12 de septiembre del 2014, tiene por objeto conforme lo señala el artículo 1 “regular los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador”, además en su artículo 3 numeral 2 señala el objetivo de proteger los derechos de los usuarios de los servicios financieros, de valores y seguros.

La protección de los datos de carácter personal no es tema de regulación del Código monetario, pero por las características de los servicios financieros es necesario para las instituciones que lo componen, el tratamiento y conservación de datos personales de sus usuarios. Por lo tanto, es necesario que exista una regulación que garantice el derecho de los titulares de los datos personales y las obligaciones de los responsables.

Se debe destacar que las entidades del sistema financiero no solo manejan datos de carácter personal relacionados con la identidad registrable de la persona, también disponen de datos patrimoniales y de historial crediticio.
El artículo 255 del Código financiero señala la prohibición de las entidades del sector financiero de comercializar las bases de datos que contengan de sus clientes. El incumpliendo de esta prohibición se considera una infracción grave en palabras del artículo 262 numeral 1, lo que se sanciona administrativamente por parte de la superintendencia de bancos con multa equivalente al 0.005% de los activos de la entidad infractora. Si bien es cierto prohíbe la venta de las bases de datos de las instituciones financieras, no hace mención de la compra de bases de datos que contengan datos personales por parte de estas instituciones.

En la misma línea el artículo 352 manifiesta que los datos de carácter personal de los usuarios del sistema financiero se encuentran protegidos y la facultad de acceso solo le pertenece al titular, salvo en las excepciones señaladas en esta ley.

A pesar de que existe en este Código el ánimo de proteger los datos personales de los usuarios del sistema financiero, no desarrollo todas las facultades contenidas en el derecho autónomo de protección de datos, como son el acceso, oposición y rectificación. No se contempla un régimen claro de protección de datos, ni la entidad competente de vigilar el cumplimiento. Considerando que la definición legal de los datos personales no es clara en el Ecuador, nos pone nuevamente ante una protección ineficaz.

3.6 Ley orgánica del sistema nacional de registro de datos públicos.

La Ley orgánica del sistema nacional de registro de datos públicos, entro en vigencia en el año 2010, con la finalidad de crear y regular el sistema de registro de datos públicos, su acceso en entidades públicas y privadas que contengan dichas bases de datos. Es necesario señalar que el objeto de esta

ley es regular los registros de datos públicos, no es una ley de protección de datos personales, sin embargo, que tienen una relación directa.

La ley de datos públicos no define a los datos de carácter personal, en su artículo 6 declara como datos confidenciales: los datos personales “como ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión…” lo cual evidentemente hace referencia a los datos sensibles, en la segunda parte del artículo menciona que también son datos personales los demás atinentes a la intimidad personal y la información cuyo público pueda atentar los derechos de las personas. La cual comete el error de categorizar en el mismo artículo tanto datos sensibles como datos de carácter personal. Por lo cual es una definición confusa.

Es importante señalar que el artículo 13 de esta ley, le da la facultad a la Dirección Nacional del Registro de Datos Públicos (DINARDAP), de determinar los datos personales que podrán ser levantados y categorizados como datos públicos. Por lo tanto, es necesario que se determine de manera clara, precisa e inequívoca la diferencia entre datos personales registrables los cuales no requieren de autorización del titular para ser tratados por instituciones públicas en el ejercicio de sus funciones y datos sensibles los cuales su tratamiento no podrá carecer de dicha autorización.

3.7 Ley orgánica de gestión de la identidad y datos civiles.

El Estado para el cumplimiento de sus fines tiene la necesidad de llevar un registro de identificación de todos los ciudadanos, por lo tanto, realiza un tratamiento de datos personales sin necesidad de contar con la autorización de los ciudadanos titulares de los datos, esto quiere decir que recopila datos por mandato de la ley.

La ley orgánica de gestión de la identidad y datos civiles tiene como objetivo garantizar el derecho a la identidad de las personas y promover la

confidencialidad de la información personal. El artículo 75 de esta ley garantiza que el acceso a la información física y electrónica por derivación del derecho a la protección de datos personales podrá darse únicamente por autorización de sus titulares, representante legal o por orden judicial.

En el Reglamento a la Ley de gestión de identidad y datos civiles encontramos la definición de datos personales más precisa del ordenamiento jurídico ecuatoriano, específicamente en el artículo 2 numeral cinco el cual menciona que son datos personales “aquellos que permiten identificar o volver identificable a una persona natural”. En esta definición se deja por fuera la relación entre la persona identificada y el identificador, pero es más concordante con la normativa internacional en materia de protección de datos personales. A pesar de ser una correcta de definición de datos de carácter personal, su aplicación se vuele ineficaz al encontrarse en el reglamento a una ley, y no en una ley específica para la materia.

En el mismo numeral 5 del artículo 2 del reglamento declara la característica de los datos personales públicos, los cuales se encuentren registrados en las bases de datos del registro civil, no pierden su calidad de datos personales, ni la titularidad la de las personas sobre ellos, denominándolos datos personales de identificaciones registrables.

A pesar de los buenos aportes al régimen de protección de datos personales contenidos en la ley orgánica de identidad y datos civiles, no contiene los lineamientos para la protección de datos personales, ya que esta no es materia de su regulación, por lo tanto, señala que será competencia de la autoridad competente elaborar estos lineamientos, los cuales en su conjunto podrá dotar al ordenamiento jurídico una mejor regulación respeto de la protección de datos personales.

3.8 Ley orgánica de transparencia y acceso a la información pública.

La Ley orgánica de transparencia y acceso a la información pública, se encuentra vigente desde el año 2004, con el fin de garantizar el ejercicio del derecho fundamental de las personas de acceder a la información pública.
Como lo hemos señalado los datos públicos de las personas, no pierden su calidad de datos personales, por lo tanto, su titularidad continúa perteneciendo a las personas a las que describe. Algunas entidades de derecho público requieren para el ejercicio de sus competencias del levantamiento, tratamiento y conservación de datos de carácter personal.

Teniendo en cuanta esta consideración, la Ley de acceso a la información pública hace una diferenciación entre la información pública, la cual se caracteriza por que su acceso estará garantizado para todos los ciudadanos de manera gratuita y transparente. Y la información confidencial la cual la define en su artículo 6 como “aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella que deriva de sus derechos personalísimos y fundamentales”. Aunque el artículo no haga referencia directa a los datos de carácter personal, por las características señaladas, limita el derecho al acceso de información pública, cuando esta información contenga datos que pueden afectar la privacidad de las personas y sus datos personales.
No se puede considerar un régimen para la protección de datos personales, continúa siendo necesario el determinar exactamente mediante una ley que son datos personales, lo cual, sumando a la limitación al acceso de información pública, podrían lograr un mayor grado de protección a los datos personales los cuales estén a cargo de instituciones públicas.

3.9 Código orgánico integral penal.

El Código orgánico integral penal (COIP), es la normativa penal vigente en el Ecuador desde el año 2014. Dentro de su articula contiene como una conducta típica, antijurídica y culpable, en su artículo 178 la violación de la intimidad la cual consiste en:

> La persona que, sin contar con el consentimiento la autorización legal, acceda, intercepta, 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.
>
> No es aplicable esta norma cuando se trate de información pública de acuerdo con lo previsto en esta ley…

Del análisis de esta norma podemos señalar que el bien jurídico protegido es el derecho a la privacidad, que el este delito cuanto con múltiples verbos rectores “acceda”, “intercepta”, “examine”, “retenga”, “grabe”, “reproduzca”, “difunda” o “publique”. No se trata un delito calificado ya que cualquier persona puede ser tanto sujeto activo, como sujeto pasivo de este delito.

Es importante señalar que la falta de una definición precisa de datos personales y datos personales públicos resulta en un artículo de contenido oscuro, pudiendo resultar en decisiones judiciales injustas.

Garantizar el derecho a la protección de datos no es un tema que se pueda lograr mediante la vía penal, si bien es cierto puede ser una herramienta útil para castigar a las personas que se apropien de manera indebida de datos personales de las personas o les dé un uso que atente contra la integridad de las personas y sus derechos, la materia penal no agotará los contenidos del derecho a la protección de datos personales.

3.10 Análisis de la normativa ecuatoriana existente

Podemos concluir de manera inequívoca que la normativa ecuatoriana es inadecuada. A pesar de reconocer en la Constitución un derecho autónomo de protección de datos personales, sus contenidos y principios no se encuentran

desarrollado por la ley. Las normas que regulan los datos personales su tratamiento, conservación y uso se encuentran dispersas en diferentes cuerpos normativos y se encuentran limitadas a un ámbito de aplicación determinado.
Las grandes deficiencias de no tener una ley específica de protección de datos personales son: No se cuenta con una definición clara y precisa de datos de carácter personal, datos personales registrables y datos sensibles y en ciertas normativas se confunde su conceptualización y se los trata de la misma manera.

Dentro de la normativa ecuatoriana no encontramos un desarrollo de los derechos ARCO de las personas sobre sus datos personales, ni de los nuevos derechos reconocidos en la normativa internacional. Tampoco existe un procedimiento para que el ciudadano ejerza estas facultades o la protección directa al derecho. Esta falta de desarrollo causa inseguridad jurídica ya que no hay un verdadero alcance al derecho de protección de datos personales, facultades y obligaciones que se desprenden del mismo derecho y las consecuencias del uso sin autorización de los datos personales.

No existe en el Ecuador una autoridad competente para vigilar y castigar el incorrecto uso de los datos personales y el cumplimento de la normativa desarrollada, por lo que en la actualidad estos datos circulan sin ningún tipo de control.

Por último, hay que mencionar que el Ecuador es uno de los pocos países de la región que no cuenta con una ley de protección de datos personales, lo que causa que se encuentre en desventaja respecto a los países vecinos. El Ecuador un Estado constitucional de derechos y justicia, donde es un deber primordial del estado el garantizar el goce efectivo de los derechos, al tener un reconocimiento constitucional del derecho autónomo de protección de datos personales es necesario una ley que garantice su protección. Es materia urgente para el legislativo el expedir una ley de protección de datos personales la cual deberá garantizar la protección del derecho de las personas, también

debe contener las facultades de decisión, acceso, rectificación, cancelación y oposición, y declare la obligación de respetar los principios para lo protección de datos. Esto con el fin no solo de proteger a las personas y su intimidad, también garantizara la existencia de las condiciones adecuadas para el desarrollo económico teniendo en cuenta la importancia comercial de los datos.

4. MECANISMOS PARA LA PROTECCIÓN DE DATOS PERSONALES Y DERECHO COMPARADO

El desarrollo internacional sobre la protección de datos personales no es una materia nueva. Podemos encontrar una evolución normativa contenida en tres generaciones de la legislación de protección de datos personales.

4.1 Evolución de la normativa Internacional.

La doctrina relativa al derecho a la intimidad va evolucionando y partiendo de un derecho pasivo que proclama la no injerencia en la vida privada (Conde, 2005, p. 27). La privacidad se relaciona directamente con la protección de datos personales. Aparece por primera vez en 1890 en Estados Unidos en artículo "*The rigth to privacy*" de los autores Samuel D. Warren y Louis D. Brandeirs. (López-Torres, 2014, p. 104), posteriormente este derecho se conoció como "*the rigth to be alone*".

Las primeras normas para la protección de datos personales surgen en la década de los sesenta y setenta predominantemente en Europa. (Negro Alvarado, 2014, pp. 4-5). La primera generación de normas relativas a la protección de datos personales se caracteriza por enfocarse en el uso de bases de datos por instituciones públicas. "no hay conciencia en esta primera generación de un uso indebido de los datos por parte de los ciudadanos, entre otras razones por que daba imposibilidad técnica" (Rebollo Delgado & Serrano Perez , 2017, pág. 30). Esto responde al elevado costo de los sistemas informáticos en la época únicamente accesible para instituciones públicas y grandes empresas privadas.

Estas normas de primera generación protegen el espacio físico donde se almacenaba la información, requiriendo autorización previa para el acceso y uso. Además, se crean instituciones encargadas de controlar el tratamiento de datos y la obligación de presentar informes del funcionamiento de equipos informáticos. Pertenecen a esta generación la Ley alemana "*Datenschutz* de *Land de Hesse"* de 7 de octubre de1970, la "*Data Lag"* de Suecia del año 1973 y la también alemana *Landesdatenschutzgesetz* del 24 de enero de 1974 del *Land de Renania-Palatinado.* (Rebollo y Serrano, 2017, p. 30)

La segunda generación de leyes fijó menos trabas para la constitución de bases de datos, pero, en contrapartida, confirieron facultades al titular de los datos (Cerda Silva, 2003), se refleja conciencia respecto a la posibilidad de que el uso indebido de los datos personales puede lesionar el derecho a la privacidad de las personas. Por lo tanto, el tratamiento de datos debe contar con una justificación. "Se establecen en esta generación los principios básicos en el tratamiento de datos, como el consentimiento del titular, el derecho de acceso y control, mantener la calidad de los datos e informar la finalidad de los mismos". (Rebollo y Serrano, 2017, pp. 30-31). Se establece también la protección adicional a los denominados datos sensibles, lo cuales en su tratamiento pueden causar mayor lesión a las personas y exponerla a prácticas discriminatorias. Las normas representativas de esta generación son el "*Privacy Act"* del año 1974 de Estados Unidos de América y las leyes de 1978 de Austria, Dinamarca, Noruega y en especial la Ley Francesa sobre informática, ficheros y libertades. (Cerda Silva, 2003)

El surgimiento en 1983 del internet y la promulgación de la sentencia del Tribunal Federal Alemán de 15 de septiembre de 1983 (Rebollo y Serrano ,2017, p. 31), que presento el concepto del derecho a la autoderminación informativa dieron surgimiento a una tercera generación de normativa para la protección de datos personales.

“El planteamiento del problema en estas fechas es sencillo, la evolución técnica y de forma concreta de las telecomunicaciones, hace posible la vulneración de derechos fundamentales con gran facilidad” (Rebollo y Serrano, 2017, p. 31).
Se hace necesario regular la protección de datos desde una visión internacional, que regule de manera unificada la protección de datos personales y la trasferencia internacional de los mismos. “Responde a esta orientación el Convenio 108 adoptado por la Comunidad Europea en 1981, primer instrumento internacional con respecto al tiramiento de datos personales, el cual establecería principios básicos para las leyes de protección de datos de los países europeos” (Cerda Silva, 2003). En Portugal se publica le Ley de protección de datos personales en 1991, en España la Ley Orgánica de tratamiento automatizado de datos de carácter personal (LORTAD), a nivel de la Comunidad Europea la Directiva 95/66/CE y la Directiva 97/66/CE y el Actual Reglamento UE 2016/ 670 (GDPR).

Sobre los mecanismos de protección de datos personales en Latinoamérica Dante Negro Alvarado menciona:

> En los países de América Latina, se han elaborados mecanismos de protección de datos personales básicamente desde el concepto del habeas data. El cual es un derecho constitucional que permite a las personas el acceso a la información personal en bases de datos públicas y privadas para corregir y actualizar los mismos, además de permitirles la posibilidad de asegurar que los datos sensibles mantengan su confidencialidad o sean retirados de dichas bases. (Negro Alvarado, 2014)

La acción de habeas data resulta por sus características ineficiente para garantizar la protección de datos personales. El habeas data no es una figura que contenga obligaciones para las instituciones públicas o privadas que manejen datos personales cuenten con un estándar mínimo para su protección. Las personas mediante al habeas data podrán acceder y conocer únicamente

respecto a su información personal y de sus bienes cuando la institución responsable se negare a permitir el acceso, la actualización o realice un mal uso de los datos personales. La protección de datos personales debe garantizarse en todo momento el cumplimiento de un estándar. La acción de habeas data entra cuando ya ha existido un daño o exista la sospecha del mismo. Debido a esto, en los últimos años la mayoría de los países de américa latina han expedid leyes específicas para la protección de datos personales. La doctora Lorena Naranjo Godoy, directora nacional del Registro de Datos Públicos (DINARDAP) en entrevista para al diario el Universo de fecha 23 de abril de 2018 afirma:

> El numeral 19 del artículo 66 de la Constitución vigente desde el 2008 estipula el derecho a la protección de datos de carácter personal. Pero aún no está regulado (en el Ecuador), igual que en otros dos países de la región: Venezuela y Bolivia. (Naranjo Godoy, Ecuador no tiene ley para proteger datos personales, 2018)

4.1.1 Derecho comparado: análisis de la normativa comunitaria europea, mexicana y colombiana

a) Reglamento de la Unión Europea 2016/697. (GDPR)

El reglamento de la Unión Europea 2016/697 (GDPR), entro en vigencia en mayo de 2016 y es de aplicación obligatoria desde el 25 de mayo de 2018, así como el cumplimiento de los requerimientos y obligaciones. (Agencia Española de Protección de Datos Personales, 2018, p. 2). Al ser una normativa comunitaria es de aplicación directa y obligatoria para todos los países miembros de la Unión Europea.

El considerando número 13 del GDPR declara que tiene como finalidad “garantizar un nivel coherente de protección de datos personales en toda la unión y evitar divergencias que dificulten la libre circulación de datos personales”.

En el artículo 1 se señala el objeto del GDPR es “establece normas relativas a la protección de las personas físicas sobre el tratamiento de datos personales y normas relativas a libre circulación de los mismos”, “protege el derecho de las personas a la protección de datos personales y “regular la libre circulación de los datos personales”. Con respecto la titularidad del derecho las autoras Lucrecia Rebollo y María Mercedes Serrano señalan:

> La **titularidad** del derecho se le atribuye el Reglamento en su art. 1 únicamente a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia. Se excluye, por tanto, a las personas jurídicas y a los fallecidos. (Rebollo y Serrano , 2017, p. 45)

Uno de los puntos principales es el ámbito de aplicación extraterritorial del GDPR contenido en el artículo 3 el cual declara “se aplica el tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no”. Esto quiere decir que cualquier persona jurídica de derecho privado perteneciente a un país dentro de la Comunidad Europea deberá cumplir con las normas del GDPR, aunque ejerza dichas activadas fuera de ella. En el mismo artículo señala también que:

> “se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de una responsable o encargado no establecido en la Unión cuando las actividades de tratamiento estén relacionados con: 1) oferta de bienes y servicios, y 2) el control de su comportamiento”

Cualquier empresa del mundo, que realice actividades económicas de oferta de bienes y servicios o de control de comportamiento (en medida que tenga lugar en la unión), deberá cumplir con el GDPR cuando exista un tratamiento de datos personales de ciudadanos que residan en la Unión Europea. Respecto al ámbito de territorialidad del GDPR y su impacto en el Ecuador, Federico Duret Gutiérrez menciona:

> Ya que el GDPR cuenta con ámbito de aplicación extraterritorial: la oferta de bienes y servicios a ciudadanos que se encuentren en el territorio de la UE, sean europeos o no, por parte de responsables y encargados del tratamiento extracomunitario conlleva que se le aplique el Reglamento Europeo. La cuestión no es baladí, ya que numerosas empresas ecuatorianas podrían estar sometidas a su regulación. (Duret Gutiérrez, 2018)

Del análisis del artículo 3 ámbito del GDPR podría aplicar para empresas en latinoamérica, siempre y cuando realicen el tratamiento de datos personales de la Comunidad Europea. Esto amplia en gran medida el alcance de esta normativa, dicho alcance no debe ser ignorado por los países latinoamericanos, los cuales deben tomar en cuenta sus estándares de protección si quieren competir en el comercio internacional.

El GDPR también ofrece un compendio de definiciones las cuales podrían ser tomadas en cuenta para la creación de una normativa nacional para la protección de datos personales, debido a su gran desarrollo y claridad en los conceptos. El artículo 4 define de manera acertada los datos personales, datos genéticos, datos biométricos y datos relativos a la salud. El significado de tratamiento, de la limitación de tratamiento, elaboración de perfiles, fichero, responsable del tratamiento, encargado del tratamiento y consentimiento del interesado, etc.

En el artículo 5 encontramos los principios relativos al tratamiento los cuales son licitud, lealtad y trasparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad y confidencialidad.

En virtud del principio de licitud el artículo 7 establece las condiciones necesarias para otorgar el consentimiento del interesado. El responsable del tratamiento de datos deberá ser capaz de demostrar que el titular de los datos

dio su consentimiento. “Además, si el consentimiento del interesado se da en contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente a los demás asuntos” (Rebollo Delgado y Serrano, 2017, p. 48). Es importante destacar que el consentimiento puede ser revertido a voluntad del titular, por lo que no causa automáticamente ilegalidad del tratamiento.

El GDRP desarrolla los derechos ARCO de los titulares de los datos personales También garantiza nuevos derechos como son el derecho al olvido y la portabilidad de los datos personales.

Define las condiciones necesarias para la transferencia internacional de datos. Regula en su articulado el régimen de responsabilidades para tratamiento, y la obligación de contar con una autoridad independiente control en cada país miembro. También hace referencia a la protección de datos desde el diseño y por defecto en su artículo 25 y considerando 78.

b) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (“Ley Mexicana”).

La Ley Mexicana para la protección de datos personales entro en vigencia el 26 de enero de 2017, el artículo 2 declara que son objetivos de esta ley: “establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición”, también el “regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales” la cual es la autoridad competente de control del régimen de protección de datos personales en México, así como también de sancionar a quien no lo cumplan.

La Ley mexicana cuenta dentro de sus definiciones un acertado concepto de datos personales. Contiene definiciones basadas en la normativa internacional

y el desarrollo doctrinario en la materia, precisan de manera clara el concepto amplio y no restrictivo de los datos personales y su diferencia con los datos sensibles.

El tratamiento de datos personales en el marco de la Ley mexicana podrá realizarse con la observancia de los principios contenidos en el artículo 16: licitud, finalidad, consentimiento, lealtad, calidad, proporcionalidad, información y responsabilidad.

Con respecto al consentimiento el artículo 21 esta ley reconoce tanto el consentimiento expreso como el tácito, “el reconocimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, este no manifieste su voluntad en sentido contrario”. Como hemos mencionado la doctrina acepta en el caso de la protección de datos “la posibilidad de que exista un consentimiento tácito cuando se lo pueda determinar cómo inequívoco cuando se haya otorgado al interesado un plazo prudencial en el que pueda tener conocimiento de que inacción implica un consentimiento” (Rebollo y Serrano, 2017, p. 120).

La Ley Mexicana reconoce y garantiza los derechos ARCO en conjunto. Además, regular el ejercicio de estas facultas el cual deberá ser un procedimiento gratuito y simplificado. El artículo 51 señala “El responsable deberá establecer un procedimiento sencillo, cuyo plazo de respuesta no podrá exceder los 20 días”.

Reconoce también el derecho a la portabilidad de datos personales, regula toda trasferencia de datos sea nacional o internacional. Para realizar trasferencia internacional de datos personales es necesario que el país receptor cuente con facultades análogas que el emisor, es decir es necesario que se cuente con un estándar similar de protección de datos.

De la Ley Mexicana se puede destacar que crea un régimen de protección de datos adecuado, sus definiciones son claras, precisas e inequívocas. Genera

un equilibrio entre los derechos de las personas y la utilización comercial de datos personales. Incluye procedimientos simples y rápidos en beneficio de los ciudadanos además de crear una autoridad competente para garantizar la protección de datos personales.

c. Ley Estatuaria 1581 de 2012, por la cual se dicta disposiciones generales para la protección de datos personales (Colombia)

La Ley Colombiana para la protección de datos personales, tiene como objeto según su artículo 1 “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos”, la Constitución de la Republica de Colombia no reconoce el derecho autónomo de protección de datos personales, los derechos contenidos y que son el ámbito de regulación de esta ley se los menciona como parte del derecho a la intimidad personal y familiar en el artículo 15 de la Constitución.

La Ley colombiana define los datos personales de forma concordante con el Convenio 108 de la Unión europea: “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas y determinables”

Los principios para el tratamiento de datos personales que hace mención la ley de Colombia se encuentran en su artículo 4 y son el principio de legalidad, finalidad, libertad, calidad, accesos y circulación restringida, seguridad y el principio de confidencialidad. El artículo 8 señala que es derecho de los titulares el conocer, actualizar y rectificar sus datos personales.

La ley le entrega la competencia de vigilar y sancionar a la Superintendencia de Industria y Comercio quienes deberán velar por el cumplimiento de la ley de protección y sancionar.

Si bien Colombia cuenta con una ley de protección de datos esta no garantiza un buen estándar de protección. No reconoce el derecho al olvido, ni a la portabilidad de datos. La supresión de los datos personales solo cabra cuando exista una violación a los derechos o principios reconocidos. No se hace mención a la protección de datos por defecto y desde el diseño.

4.1.2 Otras normas en Latinoamérica.

Además de las normas analizadas podemos mencionar otros países Latinoamérica que cuenta con una ley de protección de datos personales como son Perú, Uruguay, Argentina y Brasil. La Ley de Protección de Datos Peruana Nro. 29733 del año 2011, la cual contiene una estructura similar a la ley colombiana, con la diferencia de que, si proclama el derecho autónomo a la protección de datos personales, y ampliando el catálogo de facultades para los titulares.

La Ley de Protección de Datos Personas y Acción de Habeas Data de 2008, es la Ley Uruguaya de protección de datos personales. Es la única ley en el ámbito latinoamericano que reconoce el derecho autónomo a la protección de datos a las personas jurídicas. El recurso para ejercer los derechos de los titulares es la acción constitucional de habeas data, misma consideración se hace en la Ley Argentina de protección de datos que data del año 2000, que por su antigüedad tampoco consagra los nuevos derechos reconocidos. Una particularidad de destacar en la normativa argentina es que contempla sanciones de índole penal para quienes falsifiquen datos de carácter personal, accedan sin autorización a bases de datos o revele sin autorización información contenida en base de datos.

El 14 de agosto de 2018 promulgo su Ley de Protección de Datos de Brasil, la cual está inspirada en le GDPR y entrara en vigencia 18 meses después de la publicación de la misma (Clarke, Modet & C°, 2018). Al igual que el GDPR la ley brinda una definición amplia de datos personales, su contenido versa sobre la necesidad del consentimiento del titular para el tratamiento de sus datos y se

crea una autoridad de protección de datos personales. (De Sousa, 2018). En esta ley si encontramos los nuevos derechos desarrollados en el GDPR.

4.2 Contenido mínimo que debe contar la ley para la protección de datos personales en el Ecuador.

El Ecuador necesita expedir una ley de protección de datos personales, con el objetivo de asegurar un estándar que proteja los datos personales de las personas y que estos no circulen libremente. Una ley de protecciones de datos garantiza el derecho autónomo a la protección de datos personales y el ejercicio de los denominados derechos ARCO, así como también los nuevos derechos: al olvido y portabilidad de datos. Es necesario que esta ley tome en cuenta la normativa internacional en especial la de los países de la región y el GDPR, para que el Ecuador sea considerado un territorio seguro para la trasferencia internacional de datos. En definitiva, una ley de protección de datos en el Ecuador deberá contener un equilibrio entre la protección y las necesidades actuales del mercado.

Luego del análisis realizado en este trabajo tanto de la evolución normativa y algunas leyes de protección de datos, consideramos que los principales puntos de una ley para la protección de datos personales deben contener son:

a) **Definiciones**

La normativa ecuatoriana deberá definir de manera clara, precisa e inequívocos conceptos básicos como dato personal, datos sensibles y datos personal registrable, también base de datos y ficheros. También es necesario definir lo que entiende la ley por “tratamiento” puesto que se deberá entender en un sentido amplio todo manejo de datos personales. Esto con el fin de no tener duda respecto a toda la información que represente datos de carácter personal. Con una definición clara se generará homogeneidad en todo el ordenamiento jurídico ya que brindará claridad cuando una norma mencione datos personales.

La ley deberá definir y diferenciar también los sujetos que intervienen en el tratamiento de datos personales.

b) Principios Rectores.

La normativa de protección de datos personales deberá contener el conjunto de principios rectores para el tratamiento de datos, los cuales deberán definirse de manera precisa ya que deberán ser observados y respetados en cualquier tipo de tratamiento de datos de carácter personales, algunos de los principios que deberá contener una ley de protección de datos son:

i. Principio de licitud: el tratamiento de datos personales debe ser apegado a lo que dictamina la ley.

ii. Principio de lealtad: “el tratamiento de datos debe realizarse en base a la normativa vigente y de acuerdo a lo convenido entre el responsable y el titular” (Santos Pascual & Lopez, 2005)

iii. Principio de exactitud: los datos deberán ser exactos y actuales, deben responder con veracidad a la situación de la persona.

iv. Principio de limitación de la finalidad: los datos personales deberán ser recogidos con fines determinados, explícitos y legítimos. Respecto al principio de finalidad las autoras Lucrecia Rebollo y María Mercedes Serrano Señalan:

> Es un elemento fundamental en el tratamiento de los datos personales pues la finalidad determina, en la recogida de datos, que se cumpla además con los requisitos de la adecuación y pertinencia; durante el tratamiento la finalidad obliga a mantener ligada la utilización del dato con la finalidad que motiva su recogida. (Rebollo & Serrano, 2017, p. 143)

Si el tratamiento posterior es incompatible con el fin, debería proceder la cancelación

v. Principio de consentimiento informado: para que le tratamiento de datos sea licito, este deberá contar con el consentimiento del titular, este consentimiento, debe contar previamente con la información suficiente, necesaria y clara de la finalidad del uso y el tiempo de tratamiento de sus datos.

vi. Principio de calidad de datos: los datos tratados deberán ser exactos, correctos, completos y actualizados.

vii. Principio de limitación del plazo de conservación: el GDPR en su artículo 5 literal c, manifiesta que los datos tratados deberán ser mantenidos “de forma que se permita la identificación de los interesados no más del tiempo necesario para los fines del tratamiento, los datos personales podrán conservarse durante un periodo largo solo con fines históricos y estadísticos”.

viii. Principio de responsabilidad: los responsables de tratamiento de datos de carácter personal deberán adoptar e implementara las medidas correspondientes para el cumplimento de los principios para la protección de datos personales (INAI, 2015, p. 47)

c) Derechos de los titulares

La ley de datos personales deberá reglamentar la forma y los medios para prestar el consentimiento el cual deberá ser entregado de manera expresa.
Los derechos ARCO de los titulares de los datos personales es decir las facultades de: Acceso, rectificación, cancelación y oposición. Deberán estar garantizados dentro de la normativa, que deberá incluir un procedimiento sencillo y rápido para ejercer dichas garantías.

La normativa deberá también reconocer el derecho a suprimir los datos, y el derecho a la portabilidad de datos personales.

d) Datos personales especialmente protegidos.

La Constitución del Ecuador señala la obligación de contar con la autorización del titular para levantar datos sensibles, por el mayor riesgo que resulta su tratamiento. La ley de datos personales del Ecuador deberá contar con la enumeración de los casos en los que será posible recolectar con autorización del titular y cuando mediante ley se podrá recopilar datos personales sensibles con el fin de cumplir las obligaciones del Estado. Se debe regular condiciones para su trasferencia entre instituciones públicas y su conservación.

e) Régimen de Responsabilidades.

La ley de protección de datos personales deberá contar con la enunciación de los derechos y obligaciones de los sujetos involucrados en el tratamiento de datos personales. En general los lineamientos de seguridad que deberán ser respetados y demostrados por quien utilice o tenga a su cargo datos personales.

Es importante determinar el nivel de afectación de las acciones cometidas por los responsables, en infracciones leves, graves y muy graves.

f) Trasferencia Nacional, Internacional e interinstitucional de Datos Personales.

Como ya ha sido señalado en este trabajo los datos personales, son de gran importancia para instituciones públicas y privadas. El sector público requiere que las instituciones que lo componen realicen un cruce de información lo que podría incluir datos de carácter personal. Es por ese motivo que es necesario que estas trasferencias sean reguladas con el fin de garantizar la protección de

datos personales y que su tratamiento posterior no sea en contrario a la finalidad con la que se levantó.

Por otra parte, para el sector privado los datos personales cuentan con gran importancia económica dentro del mercado, la ley deberá señalar la necesidad de corroborar que el país destino cuando se realice una trasferencia internacional cuente con un estándar adecuado para la protección de datos personales.

g) Autoridad competente para la protección de datos personales

Se deberá establecer una autoridad independiente y competente para vigilar, reglamentar, sancionar el sistema de protección de datos del Ecuador. La autoridad será el órgano competente donde el ciudadano podrá solicitar el ejercicio de sus derechos cuando estos no sean o podrían ser violentados por los responsables. Podrá iniciar investigaciones contra entidades públicas y privadas que manejen bases de datos personales y podrá multar administrativamente en caso de incumpliendo de la normativa. La autoridad además deberá el fomentar una cultura de protección de datos en el país, capacitación para el correcto manejo de información personal y cooperar internacionalmente para lograr un estándar común de protección de datos en la región.

h) Sanciones.

Ante el posible incumplimiento de la ley o la falta de aplicación de la misma, la autoridad de protección de datos podrá sancionar con multas económicas a las instituciones que violenten o menoscaben los derechos de los titulares.

Las multas económicas deberán ser aplicadas, en conjunto con medidas enfocadas en detener los actos contrarios a ley de protección de datos, reparar el daño a las víctimas y garantizar que no exista reincidencia. Deben guardar proporcionalidad con la gravedad de la infracción.

El desarrollo normativo a nivel mundial es el producto de varios años de avance legislativo y doctrinario, por lo que la mayoría de países cuentan con un sistema de protección de datos personales. Lo que causa que el Ecuador se encuentre en desventaja en esta metería. En el Ecuador normativa para la protección de datos personales es inadecuada, dispersa e incompleta, por lo tanto, no genera una correcta protección de datos personales.

Es necesario contar con una ley de protección de datos personales para cumplir con los estándares internacionales. La ley deberá contener definiciones claras y precisas, con el fin de brindar homogeneidad a toda la legislación relativa a datos personales. La ley además debe consagrar principios para el tratamiento de datos, los cuales son de obligatorio cumplimiento.

Para ser una normativa eficaz deberá contar con un procedimiento en favor de las personas que sea simple, rápido y de fácil acceso para ejercer sus derechos y facultades. Es necesario contar con un régimen de responsabilidades y obligaciones de los sujetos intervinientes en los tratamientos de datos y contar con una autoridad independiente y competente para reglar, vigilar y sancionar el cumplimiento de la ley de protección de datos. En el momento de armar un proyecto de ley, se deberá contar en su construcción de la participación de todos los sectores intervinientes en el tratamiento de datos personales y los titulares de los mismos. Una ley de datos personales deberá ofrecer un equilibrio entre la protección de datos y las necesidades del mercado actual.

5. CONCLUSIONES

Las nuevas tecnologías de la información nos han ayudado a generar y tratar información a gran escala, velocidad y eficiencia. Mucha de esta información corresponde a datos de carácter personal, la cual es usada tanto por el sector público y privado para el cumplimiento de sus funciones. La circulación de datos personales de forma libre y sin control puede lesionar el derecho de las personas y su privacidad.

Los datos de carácter personal son la información de cualquier tipo por intrascendente o insignificante que pueda parecer y no necesariamente de carácter íntimo, que sea atribuible a una persona natural, mediante la cual se la pueda identificar. Los datos personales brindan una descripción de las personas y pueden revelar aspectos relacionar a la identidad, origen, domicilio, historial laboral, académica y profesional, además los denominados datos sensibles pueden describir aspectos más íntimos como el pensamiento, vida sexual, origen étnico, etc.

La Constitución del Ecuador reconoce el derecho autónomo a la protección de datos personales, pero en el ordenamiento jurídico no se ha desarrollado los contenidos de este derecho. El derecho autónomo la protección de datos personales consiste en la facultad jurídica de decidir en lo concerniente a sus datos personales. En función del derecho autónomo a la protección de datos personales se deriva la necesidad de contar con la autorización del titular de datos personales para tu tratamiento. En ciertos casos el mandato de la ley suple la necesidad de una autorización del titular para el levantamiento de datos, pero no se pierde la titularidad sobre ellos

El derecho autónomo de protección de datos personales garantiza a los titulares de los datos los denominadas derechos ARCO. Con la entrada en vigencia del GDPR se reconoce también nuevos derechos relacionados como son el derecho al olvido y la portabilidad de datos.

A pesar de la importancia social y económica de los datos personales, el ordenamiento jurado del Ecuador no cuenta con una ley específica sobre la materia, por lo que de manera inequívoca podemos señalar que la normativa ecuatoriana es inadecuada. Las normas que regulan los datos personales, su tratamiento, conservación y su se encuentra dispersa en normativas que no agotan sus contenidos y se encuentran limitadas a un ámbito de aplicación determinado.

Existen problemas como la falta de definición de términos básica y elemental que sean aplicables de manera trasversal en el ordenamiento jurídico. También la falta de una autoridad administrativa que ejerza su potestad de vigilancia para controlar y vigilar el uno no autorizado de los datos personales, protegiendo así los derechos de los titulares.

Ecuador forma parte de una minoría de países en la región que no cuentan con una ley de protección de datos personales. El Ecuador se encuentra en desventaja con países que si cuentan con una legislación específica para la protección de datos. Del análisis de las normas de protección de datos personales de la región, podemos concluir que la mayoría de ellas menciona que, para la trasferencia internacional de datos personales, el país receptor deberá contar con un estándar similar de protección, condición que en la actualidad el Ecuador no cumple. En la actualidad, existen normas internacionales como el GDPRA o la reciente ley de protección de datos personales de Brasil, que tiene un ámbito de aplicación extraterritorial, por el cual empresas ecuatorianas que compitan en el mercado internacional podrían ser sometidas a su regulación.

Finalmente podemos concluir que al ser el Ecuador un Estado constitucional de derechos y justicia, donde es un deber primordial del estado el garantizar el goce efectivo de los derechos, al tener un reconocimiento constitucional del derecho autónomo de protección de datos personales es necesario una ley que garantice su protección. Se debe tomar en cuenta que por la amplitud del

derecho a la protección de datos cobija a todos los derechos los cuales pueden ser violentados en el manejo de datos de carácter personal.

Esta ley deberá contener definiciones claras y precisas, desarrollar los principios para el tratamiento de datos personales, señale los derechos y obligaciones de los sujetos intervinientes el tratamiento, las sanciones ante el uso ilegal de datos personales y la autoridad competente de vigilar el cumplimento de la normativa. La ley de protección de datos en el Ecuador deberá generar un equilibrio entre los proteccionismos y las necesidades actuales del mercado.

Cabe señalar que no importa si el nivel de protección de ley es demasiado proteccionista o en su defecto es una ley bastante suave con las empresas, somos los ciudadanos los que debemos generar una cultura de protección de datos, comprender su importancia y ejercer nuestros derechos. De ninguna manera se pretende desincentivar el uso de la tecnología, sino el promover el uso responsable de ellas. Si bien la tecnología nos brinda un sin número de comodidades y beneficio, esto no puede venir atado a una intromisión en la privacidad de los usuarios.

REFERENCIAS

Agencia Española de Protección de Datos Personales. (2018). Guia Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Madrid, España. Recuperado el 13 de Diciembre de 2018, de https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

Aparicio Salom, J. (2000). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Navarra, España: Aranzadi.

Augusto Orrero, C. (2013). Una aproximación al contenido constitucional del derecho de autoderminación informativa en el ordenamiento jurídico peruano. Anuario de Derecho Constitucional Latinoamericano, 311-330.

Cerda Silva, A. (2003). Autodeterminación informativa y leyes sobre protección de datos. Revista chilena de derecho informatico, 47-75. Recuperado el 14 Diciembre de 2018, de http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14331%2526ISID%253D507,00.html

Clarke, Modet & C°. (2018). Brasil ya tiene Ley de Protección de Datos. Recuperado el 14 de Diciembre de 2018, de Clarkemodet.com: http://clarkemodet.com/es/actualidad/blog/2018/08/brasil-ya-tiene-ley-de-proteccion-de-datos.html#.XBNCYPlKjIV

Código Orgánico de la Economía Social de los Conocimientos. Registro Oficial 899 de 9 de diciembre de 2016

Código Orgánico Integral Penal. Registro Oficial 180 de 10 de febrero de 2014.

Código Orgánico Monetario y Financiero, Libro I. Registro Oficial 332 de 12 de septiembre de 2014

Conde Ortíz , C. (2005). LA PROTECCIÓN DE DATOS PERSONALES: UN DERECHO AUTÓNOMO CON BASE EN LOS CONCEPTOS DE INTIMIDAD Y PRIVACIDAD. MADRID, España: DYKINSON.

Constitución de la República del Ecuador. (2008). Registro Oficial 449 de 20 de octubre de 2008.

Convención Americana sobre Derecho Humanos. (1969). Recuperada de http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

Davara Rodríguez , M. A. (2001). Manual de Derecho Informático. Elcano: Aranzandi.

De Sousa, A. (2018, Julio 17). ¿En qué consiste la Ley General de Protección de datos recientemente aprobada en Brasil? Recuperado el 14 de Diciembre de 2018, de DerechosDigitales Derechos Humanos y Tecnología en América Latína: https://www.derechosdigitales.org/12309/en-que-consiste-la-ley-general-de-proteccion-de-datos-recientemente-aprobada-en-brasil/

Declaración Universal de Derechos Humanos (1948). Recuperado de https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Domínguez, A. G. (2016). Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua. Madrid: Dykinson.

Duret Gutiérrez, F. (2018, Junio 12). Qué debe contener una ley de protección de datos en Ecuador. Recuperado el 14 de Diciembre de 2018, de Revista Gestión Digital: https://revistagestion.ec/investigacion-analisis/que-debe-contener-una-ley-de-proteccion-de-datos-en-ecuador

Fernández Cabrera , S. (2015, Julio). El derecho al olvido. Revista Venezolana de Legislación y jurisprudencia(6), 207-235.

Frutos Mendoza, O. (2013, Marzo-Mayo). El derecho de cancelación de datos personales en archivos privados en México y España. Derecom(13), 11-27.

Grimalt Servera, P. (1999). La responsabilidad civil en el tratamiento automatizado de datos personales. Albolete , Granada, España: Comares.

INAI. (2015). Principios y deberes en materia de Protección de Datos Personales. Mexico. Recuperado el 14 de Diciembre de 2018, de http://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Princ

ipios%20y%20deberes%20en%20materia%20de%20Proteccio%CC%81n%20de%20Datos%20Personales.pdf?sequence=1&isAllowed=y

Jijema Leiva, R. (2013). Tratamiento de datos personales en el Estado y acceso a la información pública. Revista chilena de Derecho y Tecnología, 2(2), 49-94. doi:10.5354/0719-2584.2013.30309

Larrea Holguín, J. (2008). Manual Elemental de Derecho Civil del Ecuador (Vol. I). Quito: Corporación de Estudios y Publicaciones.

Ley de Comercio Electrónico, Firmas y Mensajes de Dato. Registro Oficial 557 de 17 de abril de 2002.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Registro Oficial 52 de 22 de octubre de 2009.

Ley Orgánica de Gestión de la Identidad y Datos Civiles. Registro Oficial 684 de 04 de febrero de 2016.

Ley Orgánica de Telecomunicaciones. Registro Oficial 439 de 18 de febrero de 2015.

Ley Orgánica de Transparencia y Acceso a la Información Pública. Registro Oficial 337 de 18 de mayo de 2004.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. Registro Oficial 162 de 31 de marzo de 2010.

López-Torres, J. (2014, Julio). Antecedentes Internacionales en Materia de Privacidad y Protección de Datos Personales. EAFIT. Journal of International Law(5-2), 103-117.

Ministerio de Telecomunicaciones y Sociedad de la Infomración (MINTEL). (2018). Libro Blanco de la Sociedad de la Informacion y el conocimiento (primera edición ed.). Quito, Ecuador . Recuperado el 14 octubre de 2018, de telecomunicaciones.gob.ec

Morell, J. (2014, Febrero 17). Si tus datos son el petróleo de internet,¿a dónde va a parar ese oro negro? El diario.es. Recuperado el 15 de dicimebre de 2018, de https://www.eldiario.es/hojaderouter/internet/datos-internet-privacidad-Big_Data-Jorge_Morell_0_276122595.html

Murillo de la Cueva, P. L., & Piñar Mañas, J. L. (2009). El derecho a la autoderminación informativa. Madrid: Fundación Coloquio jurídico Europeo.

Naranjo Godoy , L. (2018). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. (R. Ávila , Ed.) Foro Revista de Derecho: La protección de datos personales en la era digital(27), 63-82.

Naranjo Godoy, L. (2018, Abril 29). Ecuador no tiene ley para proteger datos personales. (D. E. Universo, Entrevistador) Recuperado el 12 de Diciembre de 2018, de https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales

Negro Alvarado, D. M. (2014, Enero). HACIA UN MARCO NORMATIVO EN LAS AMÉRICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES. Anuário Brasileiro de Direito Internacional(XI-1), 181-205.

Pacto Internacional de Derechos Civiles y Políticos (1976). Recuperado de https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

Puccinelli, O. R. (2017, Enero). El derecho a la portabilidad de los datos personales, orígenes, sentido y alcances. Pensamiento constitucional, XXII(22), 203-228.

Real Academia Española. (2017). Diccionario de la Lengua Española. Recuperado el Novimebre 05, 2018, de http://dle.rae.es/?id=LyCn6I9

Rebollo Delgado , L., & Serrano Perez , M. M. (2017). Manual de Protección de Datos (2da ed.). Madrid, España: Dykinson.

Reglamento de la Unión Europea 2016/679 (2016). Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Santos Pascual , E., & Lopez, I. (2005). Protección de datos personales, manual práctico para empresas . Madrid : FC Editorial.

Troncoso Reigada, A. (2010). LA PROTECCIÓN DE DATOS PERSONALES. EN BUSCA DEL EQUILIBRIO. Valencia, España: Tirant lo Blanch.

Uicich, R. (1999). Los Bancos de datos y el Derecho a la Intimidad (Primera ed.). (R. Villela, Ed.) Buenos Aires, Argentina : AD-HOC.

Villalba Fiallos , A. (2018, Febrero). Reflexiones Jurídicas sobre la Protección de Datos y el derecho a la Intimidad en la Autodeterminación informativa. Foro Revista de Derecho: La protección de datos personales en la era digital(27), 23-42.