UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ
Colegio de Jurisprudencia

Análisis sobre el consentimiento del titular bajo la Ley de Protección de Datos Personales

Diego José Jaramillo Intriago

Colegio de Jurisprudencia

Trabajo de fin de carrera presentado como requisito
para la obtención del título de Abogado

Quito, 20 de noviembre de 2022

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos:	Diego José Jaramillo Intraigo
Código:	00206053
Cédula de identidad:	1718614231
Lugar y Fecha:	Quito, 20 de noviembre de 2022.

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses

ANÁLISIS SOBRE EL CONSENTIMIENTO DEL TITULAR BAJO LA LEY DE PROTECCIÓN DE DATOS PERSONALES[1]

ANALYSIS OF DATA HOLDER'S CONSENT ACCORDING TO THE PERSONAL DATA PROTECTION LAW-[2]

RESUMEN

En los últimos años el derecho a la protección de datos ha cobrado gran importancia. El pilar fundamental de este derecho radica en la manifestación del consentimiento del titular de los datos. No obstante, para que este se autorice sin problema alguno se requiere de un estándar estricto y claro establecido previamente al tratamiento de los datos. En el Ecuador, el estándar de manifestación del consentimiento carece de claridad y rigidez. Por lo tanto, es necesario fortalecer el sistema actual desarrollando conceptos básicos del consentimiento y estableciendo requisitos inspirados en legislación extranjera para establecer un sistema acoplado a la realidad ecuatoriana que permita una mayor seguridad para el titular de los datos y la entidad que los recoge.

PALABRAS CLAVE

Protección de datos, datos personales, consentimiento, manifestación de la voluntad, autorización, estándar, Ley Orgánica de Protección de Datos Personales.

ABSTRACT

In recent years, the right to data protection has gained great importance. The fundamental pillar of this right lies in the manifestation of the data owner's consent. However, for this to be authorized without any problem, a strict and clear standard must be established prior to the processing of the data. In Ecuador, the standard of manifestation of consent lacks clarity and rigidity. Therefore, it is necessary to strengthen the current system by developing basic concepts of consent and establishing requirements inspired by foreign legislation to create a system coupled to the Ecuadorian reality that allows greater security for the data owner and the entity that collects the data.

KEY WORDS

Data protection, personal data, consent, manifestation of will, authorization, standard, Ley Orgánica de Protección de Datos Personales.

[1] Trabajo de titulación presentado como requisito para la obtención del título de Abogado. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por Oswaldo Santos.

Fecha de lectura: 20 de noviembre de 2022
Fecha de publicación: 20 de noviembre de 2022

SUMARIO

1. Introducción

En las últimas décadas el derecho a la protección de datos personales ha cobrado mucha importancia[3]. Los principales responsables de tan repentina relevancia son la globalización y los intensos avances tecnológicos que ocurren día a día[4]. Por esto, la protección de datos personales es una necesidad cada vez más latente en la sociedad. Incluso, sin un buen manejo de esta materia, se podrían vulnerar derechos de los titulares de los derechos inadvertidamente. El elemento principal por el cual, de manera preventiva, se evita que existan dichas vulneraciones de derecho es una correcta recolección de los datos. Para que este proceso ocurra de manera adecuada es necesario que la manifestación del consentimiento del titular de la información sea innegable. Por esto, el estudio del presente trabajo se centrará en demostrar la importancia del consentimiento en la protección de datos y cómo se presenta en el régimen ecuatoriano.

En Ecuador se ha desarrollado la Ley Orgánica de Protección de Datos Personales (en adelante LOPD) con afán de adaptarse a estas nuevas necesidades tecnológicas como la protección de nuevos derechos y principios. La ley en su primer artículo define de manera exacta su objeto y finalidad, que es "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela"[5]. En este sentido, la LOPD pretende ofrecer facilidades a las personas naturales o jurídicas para garantizar el derecho a la protección de datos personales.

[3] Aristeo García González, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín mexicano de derecho comparado* vol.40 no.120 (2007).
[4] Concepción Conde Ortiz, La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad, (Madrid: Dykinson, 2016), 19-21.
[5] Artículo 1 Ley Orgánica de Protección de Datos Personales, [LOPD], Registro Oficial No.459, 26 de mayo de 2021.

Por lo tanto, es claro el fin que tiene la protección de datos en el Ecuador y en el mundo: proteger derechos nacientes de nuevas situaciones tecnológicas. Estas situaciones esencialmente se reducen a las que nacen por la interacción entre dos personas naturales o jurídicas en la recolección y tratamiento de datos. Entre ellas podemos pensar en la aceptación del tratamiento por llamadas telefónicas, presionar un botón de afirmación o incluso con la firma de un contrato. Para lograr este fin y lidiar con estos nuevos escenarios se debe entender cuáles las partes fundamentales de la protección de datos, y principalmente la manifestación del consentimiento del titular.

Como se demostrará en las secciones siguientes la piedra angular de cualquier interacción que tenga como principal eje el tratamiento de los datos es el consentimiento de su titular. No basta cualquier consentimiento o una manifestación laxa del mismo. El estándar internacional todavía no se ha unificado por completo, pero comparte algunas características como se podrá observar a lo largo de este trabajo. En el Ecuador, en cambio, existe una especie de estándar amplio que puede prestarse a interpretaciones perjudiciales para los interesados. Por esto, a lo largo de esta investigación se planteará un mecanismo de recolección de datos más riguroso aplicable en el Ecuador para así salvaguardar derechos de los titulares y respetar principios básicos de la protección de datos.

2. Estado del arte o importancia de la recolección de datos personales

2.1. Importancia social y empresarial del tratamiento de datos personales

Los avances tecnológicos han desplegado nuevas necesidades en las relaciones entre empresas y consumidores[6]. Dentro de estas necesidades se encuentran situaciones relacionadas específicamente al tratamiento de la información de los consumidores por parte de las empresas. Dichas situaciones afectan principalmente a dos grupos en particular: los titulares de los datos y las personas naturales o jurídicas encargadas de su tratamiento. Ambos grupos tienen intereses y necesidades distintas. Por esto, surge la importancia social y empresarial de la protección de datos.

La importancia social o de las personas titulares de los datos recae en su mayoría en el derecho de ellas a la autodeterminación informativa. Dicho derecho tiene su origen de la sentencia del Tribunal Constitucional de la República Federal Alemana sobre la Ley de Censo de 1983. En

[6] José María Ayala Muñoz y Celia Fernández Aller, "La protección de datos: una necesidad", *eca Estudios Centroamericanos* vol.60 no.708 (2007), 955-960.

palabras de ese tribunal, este derecho se define como "la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona"[7], es decir, el derecho a que no se utilice la información provista por el usuario sin su consentimiento previo. Este derecho, si bien esta reconocido en distintas legislaciones latinoamericanas como Perú[8], Ecuador[9] y Colombia[10] es aplicable en la mayoría de legislaciones occidentales que tratan a la protección de datos, principalmente porque el consentimiento es la base de toda relación que tenga por objeto el tratamiento de datos de carácter personal.

No obstante, cuando no se respeta este derecho y otros ligados a la protección de datos podemos enfrentarnos a ciertos riesgos para el usuario. El riesgo que predomina en la realidad ecuatoriana y mundial es la pérdida del rastro de los datos que ocurre cuando el titular de la información no conoce el paradero de esta después de haber consentido transferirla. Esto, porque el consentimiento debe ser individual para cada fin que pueda tener su tratamiento, no obstante, el titular no tiene un verdadero control sobre los fines para los que la empresa pueda utilizar sus datos. A manera de ejemplo, una persona puede brindar sus datos al hacer una compra en una compañía de telefonía. No obstante, estos datos pueden perderse en los distintos órganos de la empresa y utilizarse para otros fines de los previstos en cualquier momento sin que la persona conozca dichos movimientos por falta de una correcta manifestación del consentimiento al inicio del proceso de tratamiento. Incluso, podría terminar en empresas con el mismo giro del negocio por filtraciones de información que no necesariamente implican un ataque informático. Entonces, bajo este supuesto se estarían violentando derechos de los usuarios, en especial, el derecho a la autodeterminación informativa porque una vez brindada la información el usuario no tiene herramientas de control sobre ella. Por lo tanto, es importante que desde el inicio del proceso de recolección este sea transparente en el que el titular de los datos tenga pleno consentimiento para entregarlos.

Por otro lado, también existe la importancia del tratamiento de datos para las entidades que los recogen. Principalmente los distintos ordenamientos recogen deberes y obligaciones

[7] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la Republica Alemana, Sentencia Constitucional, 15 diciembre 1983.
[8] EXP. N.° 00300-2010-PHD/TC, Tribunal Constitucional de Perú, Sala Segunda del Tribunal Constitucional, 12 de octubre de 2009, párr 5.
[9] Sentencia No. 2064-14-EP/21, Corte Constitucional del Ecuador, 27 de enero de 2021, párr 133.
[10] T-729/02, Corte Constitucional de la República de Colombia, La Sala Séptima de Revisión de la Corte Constitucional, 05 de septiembre de 2002.

conectados directamente con los derechos de los titulares, tratándolos como su contrapartida. Por ejemplo, para proteger el derecho a la rectificación y actualización de los datos, la empresa o entidad que solicita los datos debe proveer de un sistema amigable al consumidor para que la actualización sea inmediata. Es decir, las obligaciones de las empresas siempre estarán ligadas a un derecho que debe ser protegido.

2.2. Tratamiento y recolección de datos personales

Sobre el concepto de tratamiento de la información, la OEA en su publicación "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales" ha llegado a la siguiente definición:

> [el tratamiento de los datos] abarca toda operación o conjunto de operaciones realizado con Datos Personales, incluyendo, de manera enunciativa más no limitativa, la recopilación, acceso, organización, adaptación, indexación, aprovechamiento, registro, almacenamiento, alteración, recuperación, divulgación o transferencia[11].

Para un mejor entendimiento del alcance de este concepto, se han planteado 13 principios rectores para el tratamiento de datos personales. Entre ellos, la OEA reconoce que uno de los principales principios para el tratamiento de la información es la transparencia. Este se refiere a que la información sobre el uso de los datos personales debe ser provista al usuario de manera clara, inteligible y con un lenguaje sencillo para que proceda el tratamiento de los datos del usuario[12]. En este mismo sentido, la LOPD recoge el principio de lealtad el cual de manera literal expresa que: "para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados"[13]. Además, un elemento fundamental de este principio es que esta información debe ser accesible, comprensible y utilizando un lenguaje sencillo.

Por otro lado, y siendo un tanto más específico, el doctrinario Emercio José Aponte Núñez también ha planteado ciertos principios sobre los cuales recae la protección de datos. Entre ellos se encuentran: i) el consentimiento del titular, ii) la calidad de los datos, iii) información en la recolección de los datos, entre otros[14]. Para efectos de este escrito, el primer principio es

---

[11] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, Publicación aprobada por la asamblea general de la OEA, Organización de los Estados Americanos,
OEA/Ser.D/XIX.20, 03 de enero de 2022.

[12] Ibid.

[13] Ley Orgánica de Protección de Datos Personales, [LOPD], Registro Oficial No.459, 26 de mayo de 2021.

[14] Emercio José Aponte Núñez, "La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano Revista de Derecho Privado, ISSN-e 0123-4366, Nº. 12-13, (2007).

fundamental para conocer en qué momento el titular conscientemente autoriza de manera clara el tratamiento de sus datos. De esta forma, amparado en el Tratado por el que se establece una Constitución para Europa el autor determina que la única persona para permitir el trato de sus datos es el titular de estos[15]. No obstante, también plantea la posibilidad de que el consentimiento se manifieste de manera tácita o expresa. Por un lado, la manifestación tácita hace referencia a las acciones e inacciones que indican que el usuario está de acuerdo con el tratamiento de sus datos. Por otro, la manifestación expresa indica un modo de aceptación directo e inequívoco.

En el Ecuador, la LOPD se ha inspirado en conceptos internacionales para desarrollar derechos, principios y normas relacionadas al tratamiento de los datos de carácter personal. Ha utilizado los principios de transparencia, lealtad y legitimidad como lo ha hecho la OEA de una manera similar, centrando la importancia de dichos principios en la claridad que debe tener el portador de los datos a como se los va a utilizar, recopilar y la finalidad que tendrán. Por otro lado, también ha dado importancia a la manifestación del consentimiento del titular de los datos. No lo trata como un principio, pero como un elemento fundamental para el tratamiento de los datos. La ley, en su artículo 8 prevé 4 requisitos para que este elemento se cumpla; el consentimiento debe ser libre, especifico, informado e inequívoco[16]. Es decir, de la manera en la que presenta los requisitos dichos articulo da la impresión de que no se permite que la manifestación del consentimiento se presente de manera tácita.

3. Marco teórico

El sistema de tratamiento y obtención de datos personales en el Ecuador establecido en la LOPD es un claro ejemplo de adaptación normativa a las necesidades de la sociedad ecuatoriana. En esencia, estas nuevas necesidades se centran en el derecho a la protección de datos el cual, a su vez, está relacionado a otros derechos como el de privacidad, libertad personal, autodeterminación informativa, entre otros. Además, es importante proteger los datos personales de los titulares, sensibles o no, y los derechos inherentes a ellos.

Brindar un ecosistema seguro para el tratamiento de datos trae consigo muchos beneficios para el Ecuador. Uno de estos es la posibilidad de que crezca la inversión extranjera en el

[15] Tratado por el que se instituye una Constitución para Europa, Roma; Italia, 29 de octubre de 2004.
[16] Articulo 8, LOPD.

territorio[17]. Esto simplemente porque ven al sistema jurídico ecuatoriano como uno confiable para el manejo de sus datos siendo estos uno de los pilares de la economía e innovación de los países[18]. Internamente, la Dirección Nacional de Registros Públicos también ha establecido ciertos beneficios el su boletín oficial 252, entre ellos se encuentran: "proteger a grupos de atención prioritaria, garantizar a los ciudadanos que sus datos están protegidos de robos de identidad y estafas, brindar servicios digitales más eficientes y eficaces"[19].Por lo tanto, desarrollar una ley que regule al tratamiento, recolección y gestión de datos personales genera muchos beneficios y es cada vez más necesario para los estados.

La necesidad de los estados de establecer un sistema de protección de datos tiene su fundamento en la seguridad informática de sus nacionales. Existen algunos casos en el mundo en los que la fuga de información ha afectado a los titulares de los datos filtrados. En el Ecuador, uno de los casos que tuvo un gran número de afectados fue la fuga de información de las bases de datos de la empresa ecuatoriana Novaestrat[20]. En este caso, lo que paso es que una empresa ecuatoriana depositó enormes cantidades de información de ciudadanos ecuatorianos en servidores vulnerables en otro país[21]. Por lo que, el análisis principal es saber cómo dicha empresa consiguió todos estos datos los cuales se encontraban en diferentes entidades estatales. Una vez descartado que fue un hackeo, la opción más viable es una fuga de información a propósito, lo que es una clara violación a los derechos de los titulares y más importante al consentimiento que cada uno de ellos presto al entregar sus datos. Es por esto que este tipo de riesgos o complicaciones podrían reducirse substancialmente si el sistema de recolección y tratamiento de los datos funciona de manera correcta. Es decir, respetar el consentimiento primario de los titulares de los datos es fundamental para proteger sus derechos. Sin embargo, para poder respetarlo la normativa debe plantear un estándar claro y estricto para autorizar el tratamiento de los datos.

[17] Felipe Nicolás Roldán Carrillo, "Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador". *USFQ Law Review*, Vol. 8, no 1, (2021), 177-178

[18] Access Now, Derechos Digitales, APC. "Requisitos mínimos para la Ley de Protección de Datos Personales de Ecuador" Asociación para el Progreso de las Comunicaciones (APC), Mayo 29, 2020, https://www.apc.org/es/pubs/requisitos-minimos-para-la-ley-de-proteccion-de-datos-personales-de-ecuador

[19] Dirección Nacional de Registros Públicos, "Beneficios tras la aprobación de la Ley de Protección de Datos Personales", Boletín Oficial: 252, (2021).

[20] El Universo, "Datos a la venta dan cuenta de que filtraciones no son nuevas en Ecuador" El Universo, 21 de septiembre de 2019, https://www.eluniverso.com/noticias/2019/09/21/nota/7527550/datos-venta-dan-cuenta-que-filtraciones-no-son-nuevas/.

[21] El Universo, "Datos a la venta dan cuenta de que filtraciones no son nuevas en Ecuador"

4. Evaluación de la normativa en Ecuador

En el Ecuador, los últimos años han sido claves para el crecimiento y avance en la normativa relacionada a la protección de datos. En el 2019 se presentó el Proyecto de Ley de Protección de Datos Personales (en adelante Proyecto de Ley) siendo este el primer paso para una regulación integral sobre la protección de datos[22]. Posteriormente la ley fue publicada en el quinto suplemento del Registro Oficial No.459 , 26 de Mayo 2021. Por esto, en el presente capítulo se analizarán las particularidades referentes a la manifestación del consentimiento en el tratamiento de datos personales y de sus categorías especiales contenidas en el texto del Proyecto de Ley en contraste con el texto de la Ley publicada.

4.1. Proyecto de Ley Orgánica de Protección de Datos Personales

En el Proyecto de Ley, se incluyeron algunas regulaciones para el tratamiento de los datos personales. Entre ellas está la distinción que hace entre datos personales y sus categorías especiales. En este mismo sentido, al hacer esta distinción también plantea un trato diferenciado para ambas categorías. Además, el proyecto contempla un estándar claro y específico para que se configure el consentimiento del titular de prestar sus datos personales en estas dos clases.

Antes de comprender el tratamiento que les da el proyecto de ley es menester entender qué significa cada una de estas categorías. Por un lado, tenemos a los datos personales, que son todo: "Dato que identifica o hace identificable a una persona natural, directa o indirectamente. en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto"[23]. Por otro lado, el mismo cuerpo normativo define a los datos sensibles como:

> Se consideran datos sensibles los relativos a **etnia**, identidad de **género**, identidad **cultural**. **religión**, **ideología**, filiación **política**. pasado **judicial**. condición **migratoria**, orientación **sexual**. **salud**. datos **biométricos**. datos **genéticos** y aquellos cuyo tratamiento indebido pueda dar origen a **discriminación**. atenten o puedan atentar **contra** los **derechos humanos** o la **dignidad** e **integridad** de las personas. La Autoridad de Protección de Datos Personales podrá determinar **otras categorías** de datos **sensibles**. (énfasis añadido)[24].

[22] Proyecto de Ley Orgánica de Protección de Datos Personales. R.O. Suplemento 463 de 17 de noviembre de 2004. Proyecto de Ley Orgánica de Protección de Datos Personales, T.514-SGJ-19-0740, Asamblea Nacional de la Republica del Ecuador, Número del Registro Oficial y 19 de septiembre de 2019
[23] Articulo 5, Proyecto de Ley Orgánica de Protección de Datos Personales
[24] Ibid.

Es decir, el proyecto de ley es muy amplio en relación a lo que corresponde datos sensibles. Ahora bien, la razón para dividir ambas categorías es principalmente proteger derechos adicionales de los titulares de datos sensibles.

Una vez definidas ambas categorías es importante estudiar sus diferencias el momento de la manifestación del consentimiento de cada una por separado. El Proyecto de Ley plantea un estándar claro en el cual la manifestación del consentimiento requiere seis características esenciales, debe ser: libre, especifico, informado, inequívoco, previo y expreso. A continuación, analizaremos cada uno de los elementos bajo los conceptos del proyecto de ley.

El primer requisito contenido en el proyecto de ley es la voluntad libre de vicios. Sobre este punto, doctrinarios como Parraguez en su libro Régimen Jurídico del Contrato ha establecido que para que la manifestación del consentimiento en un negocio jurídico esté libre de vicios debe ser "sana, en tanto libre, que efectivamente expresa lo que el sujeto quiere, como resultado del proceso intelectual de generación y exteriorización"[25]. En esencia, el Proyecto de Ley se refiere a que el consentimiento del titular debe estar exento de cualquier vicio[26]. Los vicios a los que se refiere este requisito son los mismos que aplicarían en cualquier otro negocio jurídico y los mismos que se encuentran en el artículo 1467 del Código Civil (error, fuerza y dolo)[27].

El segundo requisito trata sobre la especificidad sobre los medios de recolección y el fin que utilizará el encargado del tratamiento de los datos. Estos deben ser lo más claros que sea posible y deben informarse en un lenguaje comprensible para todas las personas, principalmente para proteger derechos de los titulares contenidos en el mismo proyecto y en cuerpos normativos internacionales. Los derechos contenidos en el Proyecto de Ley se encuentran en el capítulo tercero. No obstante, el que cobra más importancia al hablar de este requisito es contenido en el artículo 23 referente a la lealtad, transparencia e información definido como el derecho a que "el titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre. 1. Los fines del tratamiento […]"[28].

El tercer requisito implica que el consentimiento del titular debe ser informado. Este principio va muy ligado con la especificidad en el tratamiento de los datos. Simplemente, hace

[25] Luis Parraguez, El régimen jurídico del Contrato (Quito: Editora Jurídica Cevallos, 2021), 70-71.
[26] Artículo 14, Proyecto de Ley Orgánica de Protección de Datos Personales
[27] Artículo 1467, Código Civil, R.O. Suplemento 104, de 20 de noviembre de 1970, reformado por última vez R.O. 526 de 19 de junio de 2015.
[28] Artículo 23, Proyecto de Ley Orgánica de Protección de Datos Personales

referencia a que el titular de los datos debe tener conocimiento pleno sobre el fin que tendrá el brindar sus datos personales. Del mismo modo, este principio trata de proteger derechos de los titulares como el de transparencia, información, etc. Además, resguarda el principio de transparencia, fundamental para la protección de datos, tal como lo establece la ley en su artículo 9[29].

El cuarto elemento inherente para la manifestación del consentimiento contenido en el Proyecto de Ley es que el consentimiento y su autorización sea inequívoca. Sobre este requisito texto analizado mantiene un estándar muy utilizado en distintas situaciones. Establece que no debe existir dudas sobre el alcance de la autorización de uso y manejo de datos otorgada por el titular[30]. Del mismo modo, el diccionario panhispánico del español jurídico define a este estándar como el "[c]onsentimiento que no admite duda o equivocación, que no es susceptible de interpretarse en varios sentidos"[31]. No obstante, es necesario aclarar que la manifestación de voluntad puede ser expresa o tácita, a pesar de que este estándar mencione que no debe existir dudas sobre la manifestación del consentimiento. De hecho, en estas mismas circunstancias el Tribunal Supremo español ha planteado que el estándar de consentimiento inequívoco: "la entidad que pretenda obtener este consentimiento inequívoco deberá arbitrar los medios necesarios para que no queden dudas de la que cesión de los datos ha sido consentida"[32]. Es decir, independientemente de que se manifieste expresa o tácitamente es indispensable que no exista duda alguna de su autorización.

El quinto requisito hace referencia al momento en el que se debe consentir para el tratamiento de los datos, este debe ser previo a cualquier acto en el que se los utilice. Dentro de este requisito, el Proyecto de Ley plantea dos momentos en los que se puede consentir el prestar sus datos personales[33]. Primero, justo en el momento en el que el encargado del tratamiento de los datos realice un acercamiento al titular. Esto puede verse ejemplificado cuando una persona hace una compra en un establecimiento que recoge su correo electrónico para enviar información de sus productos. En este supuesto, el titular puede manifestar su consentimiento antes de realizar la

[29] Artículo 9, Proyecto de Ley Orgánica de Protección de Datos Personales
[30] Artículo 14, Proyecto de Ley Orgánica de Protección de Datos Personales
[31]Diccionario Panhispánico del Español Jurídico. (Paraguay: REAL ACADEMIA ESPAÑOLA, 2016), "Consentimiento Inequívoco," https://dpej.rae.es/lema/consentimiento-inequ%C3%ADvoco
[32]Recurso de casación 5962/2008, Tribunal Supremo , Sala de lo contencioso-administrativo, 23 de enero de 2012.
[33] Artículo 14, Proyecto de Ley Orgánica de Protección de Datos Personales

compra. El segundo momento que se establece es completamente excepcional y es posterior al momento de la recopilación de datos cuando estos no se obtuvieron de forma directa con el titular.

El último elemento, y quizás el más importante para efectos de esta investigación, se refiere a que el consentimiento debe ser expreso. Este requisito, a diferencia de la manifestación inequívoca de la voluntad, sí prohíbe a que el consentimiento sea tácito. Con este requisito parece ser que la cuestión principal de un método claro para la manifestación del consentimiento queda resuelta. No obstante, como se analizará más adelante este requisito se elimina el momento de publicar el texto final de la LODP por lo que definir una manera clara para la manifestación del consentimiento adquiere importancia.

Una vez analizado el tratamiento que da el Proyecto de Ley al consentimiento sobre datos personales es clave contraponerlo con la voluntad de proveer de categorías especiales de datos personales. El Proyecto reconoce a cinco categorías especiales de datos personales. Los datos sensibles; de niños, niñas y adolescentes; crediticios; de salud; y, que constituyan parte del patrimonio del Estado en investigación científica, histórica o estadística[34]. Sin embargo, todas las categorías reciben el mismo tratamiento al momento de analizar el consentimiento del titular para que sean utilizados.

Para que se pueda dar tratamiento a las categorías especiales de datos personales se necesita de requisitos particulares. Se deben cumplir las condiciones normales de manifestación del consentimiento contenidos en el artículo 14. Además, la norma establece que el consentimiento sea explicito. Esto se debe entender como: "aquel que puede ser demostrado de manera indubitable por el responsable o encargado del tratamiento de datos personales, en relación a la autorización otorgada por el titular a través de una declaración o acción clara y afirmativa"[35]. Evidentemente el consentimiento de este tipo de datos tiene un estándar más riguroso, debe darse por un acto claro y expreso que no permita interpretación. También, es importante aclarar que en caso de datos de niños y niñas y adolescentes que tengan menos de 16 años el encargado de permitir el tratamiento de sus datos son sus representantes legales.

El objetivo principal de esta sección es contrastar el estándar para la manifestación del consentimiento que propone el proyecto con el que fue publicado en la LODP. Por un lado, en lo referente a datos personales el estándar explicado previamente es claro y no permite

[34] Artículo 38, Proyecto de Ley Orgánica de Protección de Datos Personales
[35] Artículo 39, Proyecto de Ley Orgánica de Protección de Datos Personales

interpretaciones amplias. Por otro lado, con respecto a los datos sensibles, plantea un modo de tratamiento mucho más riguroso con el fin de reafirmar la importancia que esta categoría requiere. A continuación, se analizarán las diferencias que existen con la Ley Orgánica de Protección de Datos Personales publicada en el 2021.

4.2. Ley Orgánica de Protección de Datos Personales

La LOPD fue el avance real más contundente que tuvo el sistema normativo ecuatoriano en esta materia. Si bien el Ecuador fue de los últimos países en Latinoamérica en adoptar una ley propia sobre este tema, recibió la misma inspiración que diversos países de Latinoamérica para realizarla. Esta inspiración proviene directamente del Reglamento General de Protección de Datos realizado por el Parlamento y el Consejo Europeo el 27 de abril de 2016[36]. Con este antecedente, se presentó el proyecto de ley analizado en la sección anterior. Posteriormente, recibió algunos cambios y fue publicado el 26 de mayo de 2021.

Con este contexto, es importante delimitar el ámbito de estudio que se dará a este cuerpo normativo. De la misma manera que con el Proyecto de Ley analizado previamente, el eje central para estudiar será la manifestación del consentimiento del titular de los datos en este contexto. Por lo tanto, primero debemos analizar los requisitos que plantea la ley para que pueda configurarse el consentimiento del titular de los datos. En su artículo 8 la ley establece que la validez del consentimiento depende del cumplimiento íntegro de todos los siguientes requisitos: consentimiento libre, especifico, informado, e inequívoco[37].

La ley mantuvo los 4 primero requisitos establecidos en el proyecto de manera exacta. El consentimiento libre hace referencia a cualquiera de los vicios que este puede tener (error, fuerza y dolo). A propósito, sobre este primer requisito es importante aclarar que la norma no establece cuáles son los vicios que afectan al consentimiento en la recopilación de datos. No obstante, mediante una interpretación del ordenamiento en general podemos concluir que son los establecidos en el Código Civil[38]. Por otro lado, la especificidad se refiere a una determinación concreta de los medios y fines del tratamiento de los datos. El requisito de información pretende proteger al principio de transparencia contenido en el artículo 10 letra c) de la LOPD[39]. Además,

[36] Reglamento (UE) 2016/679, Parlamento Europeo Y El Consejo De La Unión Europea [relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE], L 119/1, de 27 de abril de 2016
[37] Articulo 8, LOPD.
[38] Articulo 1467, Código Civil
[39] Articulo 10, LOPD

incluye la necesidad de que el consentimiento sea inequívoco, haciendo referencia a que no existan dudas del alcance de la autorización del titular. En este último punto, también es importante aclarar que no se restringe en lo absoluto que el consentimiento se proyecte de manera tácita.

Los últimos 2 requisitos propuestos en el Proyecto de Ley (previo y expreso) no fueron incorporados en la ley. Esta es una de las principales diferencias con la Ley actual y genera el problema que mediante este trabajo se pretende resolver. El eje de la problemática recae en que un requisito indica que el consentimiento se proyecte de manera inequívoca pero la ley no establece un estándar claro de manifestación de tal consentimiento. Simplemente propone que este no presente dudas sobre el alcance de la autorización, siendo este un estándar más laxo a lo que se observa en el Proyecto de Ley. El plantear un estándar más flexible para la manifestación del consentimiento presenta algunos problemas. Principalmente dichos problemas se podrían presentar por una interpretación errada de los conceptos ampliamente definidos en la ley. Uno de los dos posibles problemas más importantes es una potencial vulneración de derechos como la autodeterminación informativa, el derecho a la protección de datos, e incluso la privacidad[40]. Por otro lado, el segundo problema identificable son las sanciones que podrían recibir las entidades recolectoras de los datos al no basar el consentimiento de sus titulares en un estándar rígido e inequívoco. A propósito, es importante aclarar que la razón de que exista un estándar más riguroso que el abordado por la LOPD es una solución preventiva a cualquier posible complicación que pueda surgir.

La LOPD también realiza una diferencia en el tratamiento entre datos personales y sus categorías especiales. Esto no es único en la región; de hecho, a lo largo de la mayoría de los ordenamientos jurídicos latinoamericanos existe esta distinción de categorías. Por ejemplo, la Ley 1581 de Colombia incluye en su título tercero a las categorías especiales, siendo estas los datos sensibles y lo datos personales de los niños, niñas y adolescente"[41]. En el sistema ecuatoriano esta distinción se encuentra en el artículo 25 numeral a de la LOPD enumerando a las categorías especiales de la siguiente manera: "a) Datos sensibles; b) Datos de niñas, niños y adolescentes; c)

[40] Susan Chen Mok, "Privacidad y protección de datos: un análisis de legislación comparada". Diálogos Revista Electrónica de Historia 11 (febrero 2010): https://revistas.ucr.ac.cr/index.php/dialogos/article/view/6111/13852.
[41] Ley 1581 de 2012 [Por la cual se dictan disposiciones generales para la protección de datos personales.], octubre 17, 2012.

Datos de salud; y, d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad"[42].

Si bien en el Ecuador también existen ambas categorías, el manejo de ellas es muy restrictivo. Para su tratamiento, la Ley aparentemente incluye a todas estas categorías bajo la denominación de datos sensibles. Sobre el manejo de ellos la ley es clara al mencionar que: "Queda prohibido el tratamiento de datos personales sensibles […]"[43]. No obstante, plantea ciertas excepciones en las que sí se puede utilizar los datos como cumplimiento de obligaciones, protección de intereses vitales del titular, interés público, entre otros. Esta es una distinción drástica con lo que se aprecia en el Proyecto de Ley. La LOPD es tajante al prohibir el uso de estos datos en situaciones normales, mientras que, en el Proyecto de Ley se permitía su uso con un estándar de manifestación del consentimiento mucho más estricto.

5. Marco jurídico o evaluación de normativa en otros países

El avance tecnológico en el mundo ha obligado a distintos países a crear e innovar dentro de sus legislaciones para poder cubrir nuevas problemáticas. Respecto a la protección de datos, Europa es precursor de la normativa que inspiró a la mayoría de los países de Latinoamérica a crear una normativa propia de esta materia. El Reglamento General de Protección de Datos, el cual entro en vigor en el 2018, fue la ley más completa y actualizada para la época. No obstante, previo a este cuerpo normativo ya existieron iniciativas en la región cuyo objetivo principal era proteger el derecho a la protección de datos. Por ejemplo, en 1997 se creó la Directiva 95/46/CE del Parlamento Europeo y del Consejo fue el primer acercamiento integral que tuvo la normativa de protección de datos europea.

Por otro lado, Latinoamérica también tuvo un avance importante posterior al europeo. Chile, en 1999 fue el primer país de la región en crear una ley propia de protección de datos personales. Sin embargo, el progreso más notorio con respecto a innovación normativa no se verá sino hasta el 2012 con la Ley de Protección de Datos Personales o Ley 1581 de 2012 en Colombia. Esta norma si bien obtuvo una gran inspiración del Reglamento General de Protección de Datos también incluyo nuevas disposiciones que atienden a las necesidades de su entorno social. Por ejemplo, la Ley colombiana define y atribuye un tratamiento diferenciado a los datos sensibles[44].

[42] Artículo 25, LOPD.
[43] Artículo 26, LOPD.
[44] Política de Tratamiento y Protección de Datos Personales, DS-E-GET-01 Versión 03, Ministerio De Ambiente y Desarrollo Sostenible de Colombia, 25 de julio de 2022. 13-21

Por el contrario, la ley europea no excluye a que se dé un tratamiento diferenciado, pero no propone uno como tal[45].

Del mismo modo, Perú en el 2011 decidió publicar la Ley N° 29733 o Ley de Protección de Datos Personales[46]. No obstante, la particularidad sobre la protección de datos en este país se da dos años más tarde cuando se publica el reglamento a la ley[47]. Fundamentalmente, la Ley prescribe nociones básicas de ciertos conceptos. A manera de ejemplo, en su artículo 13 numeral 5 menciona que: "Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco"[48]. Sin embargo, no existe una definición clara de todas estas características en el resto del cuerpo normativo. Por lo tanto, el reglamento entro en vigencia para suplir estos vacíos y proteger de manera óptima derechos de los sujetos que intervengan en situaciones de protección de datos.

El estudio de estas tres normativas es fundamental para comprender el impacto que ha tenido la legislación extranjera en el contexto ecuatoriano. Por un lado, la normativa europea brindó nociones básicas e iniciales sobre la protección de datos, sus principios rectores y los derechos inherentes a la materia. Por otro lado, la normativa colombiana adopto conceptos básicos del Reglamento (UE) 2016/679 pero logro adaptarse a las necesidades sociales y actuales del país. En esa misma línea, Perú creó una ley que necesitaba desarrollo en ciertos temas fundamentales por lo que en un periodo de tiempo corto se promulgó el reglamento a la misma cubriendo estos vacíos. Por esto, se analizará cada una de estas jurisdicciones para obtener un contexto más globalizado de la protección de datos.

5.1. Unión Europea: Reglamento (UE) 2016/679

El objetivo principal de la creación del Reglamento General de Protección de Datos (RGDP) es unificar los principios y la visión de la protección de datos en la Unión Europea. Por esto, dicho cuerpo normativo tiene carácter regional y de reglamento por lo que resultan vinculantes para los estados firmantes que formen parte de la región. Además, no permite tanta

[45] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo [RGDP], (UE) 2016/679, El Parlamento Europeo y el Consejo De La Unión Europea, 27 de abril de 2016.
[46] Ley 29733 de 2011 [Ley de Protección de Datos Personales], 29733, 03 de julio de 2011.
[47] Reglamento De La Ley No 29733 Ley De Protección De Datos Personales, Decreto Supremo Nº 003-2013-JUS, Congreso de la República de Perú, 22 de marzo de 2013.
[48] Artículo 13, Ley 29733 de 2011.

flexibilidad a cada uno de los países por lo que se cumple con el objetivo de uniformidad normativa a lo largo de toda la Unión Europea. Además, existen herramientas para lograr que se cumpla con esta normativa como por ejemplo sanciones. Las sanciones por incumplimiento están dirigidas a los particulares de cualquiera de estos países y estas oscilan entre los "20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía"[49].

Esto fue exactamente lo que ocurrió con la empresa Google a mediados del año 2022. La Asociación Usuarios Financieros (ASUFIN) es una empresa española que decidió presentar un reclamo ante Agencia Española de Protección de Datos (AEPD). La AEPD es la encargada de la regulación y protección de datos en España, no obstante, el régimen jurídico aplicable es el Reglamento de la Unión Europea sobre protección de datos. La reclamación presentada tiene como fundamento principal que Google violó las normas regionales para la protección de datos personales[50]. Específicamente, durante el proceso de otorgar el consentimiento para el tratamiento de los datos personales el momento de crear una cuenta de Gmail. La denuncia de ASUFIN explica que en el proceso de creación de cuentas:

> sé consiente de forma prácticamente ilimitada, el tratamiento de: uso de fecha de nacimiento, intervalo de edad y sexo, para perfilar y ofrecer anuncios y recomendaciones, así como el registro de actividad en Google, YouTube y Maps, con los fines descritos (fundamentalmente, personalización de anuncios)[51].

Además, los usuarios no tienen la facilidad para negar su consentimiento en ciertos rubros por la falta de claridad que tienen los paneles de información de la empresa[52]. Todo esto, implica violaciones serias al Reglamento de Protección de Datos.

Mientras que esta denuncia sigue tratándose en la Agencia Española de Protección de Datos, ya existen decisiones similares que protegen la eficacia del Reglamento. Un ejemplo claro de esto es la denuncia impuesta en contra de la empresa de conectividad a internet TIM ante la

[49] Art 83 RGDP.
[50] Redacción Confilegal, "ASUFIN denuncia a Google ante Protección de Datos por irregularidades en la creación de cuentas de correos", Confilegal, 05 de octubre de 2022, https://confilegal.com/20221005-asufin-denuncia-a-google-ante-proteccion-de-datos-por-irregularidades-en-la-creacion-de-cuentas-de-correos/.
[51] Asociación de Usuarios Financieros, "Denunciamos a Google ante la AEPD por irregularidades en la creación de cuentas Gmail", ASUFIN, 05 de octubre de 2022, https://www.asufin.com/denuncia-google-aepd-cuentas-gmail/.
[52] José García, "Una asociación de usuarios denuncia a Google por ignorar la ley de protección de datos en Gmail", xataka, 06 de octubre de 2022, https://www.xataka.com/empresas-y-economia/asociacion-usuarios-denuncia-a-google-ignorar-ley-proteccion-datos-gmail.

Autoridad de Control Italiana[53]. Esencialmente lo que ocurrió con esta compañía fue que realizaron campañas de marketing a alrededor de 13 millones individuos que no habían prestado su consentimiento para el tratamiento de sus datos[54]. Por otro lado, mantenían bases de datos de información de sus clientes las cuales las utilizaban para otros fines distintos a los que se especificó el momento de su recolección[55]. Estas actitudes violan derechos fundamentales de la protección de datos contenidos en el RGDP como el derecho a la información[56] y el derecho de supresión también llamado derecho al olvido[57]. En ese orden de ideas, es evidente que la compañía violento el derecho a la autodeterminación informativa el cual de él se desprende la mayoría de derechos contenidas en el Reglamento. Por esto, la Autoridad de Control Italiana ordenó el pago de 27,8 millones de euros junto con otras medidas para asegurar el cumplimiento futuro de las disposiciones de la norma[58].

Los casos previamente presentados nos ayudan a ilustrar principalmente que la norma europea tiene ciertas falencias. En específico, estas falencias radican en la manifestación del consentimiento del titular para el tratamiento de sus datos. Así lo explican Philip N. Howard, Steve Jones, el principio de consentimiento junto con la información inequívoca son la piedra angular de la protección de datos, obligando así, que exista consentimiento del titular para cada fin conocido que tenga el tratamiento de sus datos[59]. Es decir, cuando se obtiene un correcto consentimiento al inicio de la relación negocial de datos personales se podrían evitar problemas posteriores. Empero, para que exista una correcta manifestación del consentimiento la ley debe brindar las herramientas necesarias para ello.

El Reglamento comprende correctamente esta necesidad y establece con claridad la manera correcta en la que debe presentarse el consentimiento del interesado. En su artículo 4, numeral 11 define al consentimiento como: "toda manifestación de voluntad libre, específica,

[53] Lucien Zandilli, "La Autoridad de Control italiana, Garante, ha multado con 27.802.496 euros a TIM S.p.A por repetidos tratamientos ilegítimos de datos con fines de marketing", aphaia, 17 de febrero de 2020, https://aphaia.co.uk/es/2020/02/17/la-autoridad-de-control-italiana-garante-ha-multado-con-27-802-496-euros-a-tim-s-p-a-por-repetidos-tratamientos-ilegitimos-de-datos-con-fines-de-marketing/.
[54] Medida correctiva y sancionadora contra TIM S.p.A 9256486, Garante de la Protección de Datos Italiano, 15 de enero de 2020.
[55] Ibid., 2-13.
[56] RGDP, art 13.
[57] RGDP, art 17.
[58] Lucien Zandilli, "La Autoridad de Control italiana, Garante, ha multado con 27.802.496 euros a TIM S.p.A por repetidos tratamientos ilegítimos de datos con fines de marketing".
[59] Philip N. Howard, Steve Jones, Sociedad on-line: internet en contexto (Barcelona: Editora UOC, 2005).

informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (énfasis añadido)[60]. Con esta definición podemos ver que se establecen 5 requisitos claros para la manifestación del consentimiento: libertad, especificidad, información, consentimiento inequívoco y explicitud. Sobre esto, autores como Troncoso[61], Rebollo y Serrano[62] han sustentado que el estándar de manifestación del consentimiento comprende los requisitos establecidos en el artículo anterior. No obstante, este estándar no es restrictivo, de hecho, si se incluye algún otro requisito que facilite la identificación del consentimiento este debe ser aceptado.

5.2. Colombia: ley estatutaria 1581 DE 2012

La normativa de protección de datos colombiana, al igual que el resto de Latinoamérica, obtuvo su inspiración en diversos hitos de la normativa europea. Desde los primeros acercamientos a la protección de datos como derecho de los titulares en la llamada "Ley del Censo" de 1982 hasta el Reglamento General de Protección de Datos emitido en el 2016. Todo esto influyó en que Colombia desarrolle un sistema jurídico propio que verse sobre la protección de datos personales. Esto con el afán de adaptarse a las nuevas necesidades tecnológicas y sociales del país con una normativa innovadora. Por esto, en octubre del 2012 se publicó la ley 1581 "Por la cual se dictan disposiciones generales para la protección de datos personales"[63].

No obstante, es importante mencionar que la ley 1581 no es la primera normativa que pretende dar importancia y protección a datos o información de las personas. En la ley 1266 del 2008 ya se incluyeron nociones de protección de información. Pero, dicha información fue restrictiva, se centraba únicamente en datos de carácter comercial, económico y financiero. Posterior a esto y viendo que la normativa brindaba resultados de aplicación eficaces se decidió aprobar una Ley que sea más general siguiendo los lineamientos internacionales de la protección de datos personales. La ley estatutaria 1581 de 2012 la cual fue reglamentada de manera parcial por el Decreto Nacional 1377 de 2013[64].

---

[60] RGDP, art 4.
[61] Antonio Troncoso Reigada, La Protección de Datos Personales. En búsqueda del equilibrio, (Madrid: Tirant Lo Blanch, 2011).
[62]Lucrecio Rebollo Delgado y María Mercedes Serrano Pérez, Introducción a la Protección de Datos (Madrid: Dykinson, 2008), 126-128.
[63] Ley 1581 de 2012 [Por la cual se dictan disposiciones generales para la protección de datos personales.], 17 de octubre de 2012.
[64] Natalia Hernández Lotero "Clasificación de los datos personales e implicaciones legales", en Universidad Pontificia Bolivariana (Medellín, 2018), 7-8.

Con respecto al consentimiento, la normativa colombiana se diferencia de los ordenamientos ya estudiados y lo trata como autorización. En su artículo 3 titulado definiciones incluye la de la autorización en su primer numeral definiéndolo como: "Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales."(énfasis añadido)[65] Este artículo, si bien es una definición, ya plantea 3 requisitos necesarios para que la autorización sea eficaz. Por un lado, el consentimiento previo se refiere a que solo se puede obtener "a más tardar en el momento de la recolección de sus datos"[66]. Mientras que, por otro lado, el consentimiento expreso e informado se reduce a "que el dueño de la información apruebe y sepa para qué y cómo se utilizará dicha información"[67]. Es decir, todo se reduce en el consentimiento claro del fin que tiene el tratamiento de los datos.

A propósito, sobre estos requisitos, el Decreto Nacional 1377 de 2013 que pretende reglamentar parcialmente a la ley hace una explicación más profunda de la configuración de la autorización. En su artículo 5 define a la autorización como:

> El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento[68].

En otras palabras, el reglamento comenta sobre los mismos requisitos y los aclara para que no quepa duda de cómo se debe configurar la autorización. Además, el articulo 7 de la misma norma prescribe "Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización"[69]. Por lo que, mediante un análisis general de la norma podemos ver que el método para la configuración de la autorización es claro, incluso más claro que la legislación analizada anteriormente.

De esta forma, la jurisprudencia colombiana igual ha resaltado a estos requisitos como esenciales para que se configure el consentimiento y consecuentemente la autorización del titular. En el caso en que la Dirección de Investigación de Protección de Datos Personales inició un proceso de indagación a la sociedad SCOTIABANK COLPATRIA S.A se comprobó que

[65] Ley 1581, Art 3.
[66] Decreto 1377 DE 2013, Presidente de la República De Colombia [Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado], 27 de junio de 2013.
[67]Formatos Modelo Para el Cumplimiento de Obligaciones Establecidas en la Ley 1581 de 2012 y Sus Decretos Reglamentarios, Ministerio de Industria y Turismo, 2018.
[68] Artículo 5, Decreto 1377 DE 2013.
[69] Ley 1581, Art 7.

incumplió con la normativa de protección de datos. El Banco Colpatria incurrió en 3 grandes fallas que derivaron en la violación de derechos de los titulares. Primero, no atendió a tiempo la solicitud de uno de sus clientes a ser informado sobre el medio utilizado para obtener su información. Segundo, no respondió a la petición de su cliente a ser olvidado de sus bases de datos. Tercero, demostró una falta de diligencia y de responsabilidad a esta situación demorándose 20 meses en atender a estas solicitudes. Estos hechos, además de demostrar violaciones a derechos del titular como el derecho al olvido y a la información, demostró que no existía consentimiento del titular para prestar sus datos. De hecho, con investigaciones posteriores se dieron cuenta que el momento de presentar la solicitud para el tratamiento de los datos el cliente había señalado explícitamente la casilla "NO".

Este tipo de casos son similares a los que se analizaron el momento de estudiar al régimen jurídico europeo. Es decir, a pesar de tener un sistema más estricto y definido para la determinación del consentimiento del titular aun así existen falencias. Sin embargo, no necesariamente la existencia de violaciones a la norma significa que la ley tenga fallas. De hecho, en Colombia al igual que en Europa las multas no nacen por desconocimiento de la norma o por faltas simples. En realidad, la principal razón de estas fallas es la falta de diligencia de las empresas para recolectar datos. Del mismo modo, los encargados de recolectar la información no plantean la importancia que merece el consentimiento y a menudo consideran que el consentimiento único es suficiente para diversas situaciones.

5.3. Perú: Ley de protección de datos personales (No 29733) y su reglamento (Decreto Supremo No 003-2013-Jus)

En Perú, el tema relativo a los datos personales y a todos los derechos que giran en torno a él es una discusión que tiene años siendo tratada. La normativa vigente tiene 11 años de su entrada en vigor por lo que ha transcurrido suficiente tiempo para notar la eficacia de la norma en la realidad peruana. Por esto, dos años después de su entrada en vigencia, realizando un trabajo preventivo y no reactivo a cualquier complicación que pueda surgir, se publicó el reglamento a la ley. El objeto de dicho reglamento es claro y según su artículo primero consiste desarrollar la Ley de la siguiente manera: "regulando un adecuado tratamiento, tanto por las entidades públicas, como

por las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio"[70].

Esta norma, al igual que todas las analizadas anteriormente, comprenden que el inicio de toda relación negocial con objeto de protección de datos nace con el consentimiento del titular. Es tanta la importancia que la norma peruana le otorga al consentimiento que lo clasifica como un principio rector de la protección de datos. Su artículo 5 afirma que para que exista y se configure cualquier tratamiento de datos personales debe ser mediar el consentimiento del titular sin excepción[71]. Por esto, la norma plantea los siguientes requisitos inspirados en el Reglamento Europeo: el consentimiento debe ser previo, informado, expreso e inequívoco[72].

Sobre estos requisitos la normativa no elabora mucho cada uno de ellos. Pese a la falta de explicación en la norma, el reglamento fue ideal para elaborar estos conceptos. El reglamento implementa un requisito extra el de libertad, este implica que el consentimiento no tenga ningún vicio, específicamente que no "medie error, mala fe, violencia o dolo"[73] en la manifestación del consentimiento. Posteriormente, desarrolla los requisitos establecidos en la ley, sobre el consentimiento previo este se refiere a que se debe dar con anterioridad a la recolección y al tratamiento de los datos. Sobre el requisito de información, la norma requiere que se comunique clara, expresa e indubitablemente la información relevante para el titular además de utilizar un lenguaje sencillo para ello[74]. Por último, el reglamento trata a los requisitos del consentimiento expreso e inequívoco como uno solo. A breves rasgos, este requisito se cumple cuando el consentimiento "haya sido manifestado en condiciones que no admitan dudas de su otorgamiento"[75]. Del mismo modo, plantea que la condición de que este sea expreso cuando de

[70] Artículo 1, Decreto Supremo No 003-2013-JUS, Congreso de la República de Perú [Reglamento De La Ley No 29733 Ley De Protección De Datos Personales], 22 de marzo de 2013.
[71] Ley N° 29733, art 5.
[72] Ley N° 29733, art 13.
[73] Artículo 12, Decreto Supremo No 003-2013-JUS.
[74] Ibid. El reglamento ejemplifica de manera no taxativa información básica para el que el consentimiento sea informado. Entre ellos están los siguientes literales:
a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.
e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
g. En su caso, la transferencia nacional e internacional de datos que se efectúen.
[75] Artículo 12, Decreto Supremo No 003-2013-JUS.

manera oral o escrita el titular exteriorizo de manera innegable su voluntad para que el encargado de recolectar sus datos los utilice.

Como se pudo observar en esta sección, la norma peruana sí presenta nociones básicas de principios y derechos que pertenecen al régimen de protección de datos. No obstante, el reglamento a la ley fue necesario para entender y elaborar ciertos conceptos. De hecho, en la parte más importante del tratamiento de datos personales fue importante para comprender los requisitos necesarios para la manifestación del consentimiento. A manera de comparación, el régimen ecuatoriano también realiza esta extensa explicación de los requisitos para la configuración del consentimiento. Por esto, es indudable la influencia que tiene la normativa extranjera en la creación de la ley ecuatoriana, específicamente las analizadas en este capítulo.

6. Recomendaciones

Como se señaló en las secciones precedentes, el consentimiento es la base de toda interacción que tenga como eje el tratamiento de datos. Por esto, todas las legislaciones estudiadas hacen hincapié en este tema estableciendo estándares propios de cada país. Si bien cada legislación plantea sus propios requisitos para el tratamiento de los datos personales la mayoría de las legislaciones comparten algunos de ellos.

En el caso de Ecuador, los requisitos establecidos en la LOPD no son suficientemente contundentes para prevenir algún tipo de interpretación errada de ellos. Por esto, es necesario que exista un fortalecimiento de conceptos o incluso una reestructuración de los requisitos similar a lo que se pretendía en el Proyecto de Ley. La vía idónea para establecer cualquier solución es plantearlo en un posible reglamento a la LOPD. Esto aseguraría rapidez en su expedición y seguridad en su contenido. Para establecer un estándar más rígido en la manifestación del consentimiento existen dos soluciones posibles que se desarrollarán a continuación.

Primero, tomando la influencia del sistema jurídico peruano, que el posible reglamento a la Ley establezca una explicación extensiva de cada uno de los requisitos planteados en la Ley. Sobre la voluntad libre de vicios, establecer lo que los demás cuerpos normativos del país reconocen como vicios al consentimiento. Sobre la especificidad en el tratamiento de los datos, se debe aclarar que cada finalidad y que cada uso que se le dé a los datos debe autorizarse con un consentimiento especifico. Sobre el consentimiento informado de la finalidad de los datos, desarrollar que no basta con una explicación corta y poco detallada. Por el contrario, debe

informarse detalladamente la finalidad que tendrá el tratamiento de los datos del titular, utilizando, además, un lenguaje simple y comprensible para cualquier individuo. Por último, sobre el carácter inequívoco del consentimiento, establecer supuestos comunes en los que se considere que el consentimiento tiene esta característica.

Es de suma importancia que este último requisito del consentimiento inequívoco sea realmente claro. Por esto, es pertinente presentar algunos ejemplos que pueden presentarse de manera cotidiana en los cuales se asume que los demás requisitos se cumplieron previamente. Primero, para que la aceptación mediante llamada telefónica se considere innegable debe estar previamente grabada y debe existir una palabra de afirmación ("sí", "de acuerdo", "efectivamente", etc.) hacia la petición para el uso de los datos. En el supuesto en el que la aceptación implique el señalar una casilla esta debe tener sus opciones claras, es recomendable que se reduzcan a solamente dos opciones, una positiva y una negativa para evitar interpretaciones. Finalmente, en caso de que el consentimiento se configure por la firma de un documento el titular debe haber revisado diligentemente el documento y la entidad recolectora de los datos debe proveer un espacio claro y evidente dentro del documento donde realizar la firma. Cabe aclarar que estos ejemplos no son restrictivos de ninguna manera, el consentimiento se puede manifestar de otras maneras, pero debe contener la misma característica de que la manifestación de este es innegable.

La segunda posible solución para asegurar un estándar más claro y rígido en la manifestación del consentimiento implica añadir requisitos adicionales. Esta medida pretende establecer un régimen similar al que se planteó en el Proyecto de Ley. Primero, añadir el requisito por el cual se explica que el consentimiento debe obtenerse de manera previa al tratamiento. Segundo, establecer que el consentimiento debe ser expreso. Mediante este requisito no se debe entender que estrictamente sea por escrito, puede configurarse de otras maneras, pero estas deben ser indubitables y que se refieran directamente a autorizar el uso de sus datos personales. Con esos dos requisitos se fortalece la importancia que tiene el consentimiento en las relaciones que tienen por objeto el tratamiento de datos.

Es importante destacar que ninguna de las dos soluciones son restrictivas. Se podrían adoptar a la vez y resultaría aún más beneficioso. No obstante, con cualquiera de ellas se estaría cumpliendo el objetivo de este trabajo de investigación que es solucionar la falta de un estándar de manifestación del consentimiento del titular claro y eficaz. Al obtener un consentimiento claro

e innegable se asegura una correcta utilización de los datos y, como se explicará posteriormente, una protección a los derechos fundamentales a la materia.

7. Conclusión

Mediante la creación de normativa en cada país se puede inferir que la protección de datos personales y los derechos derivados de ella han ganado importancia en los últimos años. Sin embargo, la pieza fundamental para el correcto tratamiento de datos e información es el consentimiento. Este debe tener características fundamentales que, como se observó, pueden ser distintas en cada país. Sin embargo, mantienen requisitos comunes como la necesidad de que el consentimiento este informado y el titular conozca el fin del tratamiento de sus datos. También, el que el consentimiento sea expreso o inequívoco significa que no debe caber duda de que su autorización existe. Estos junto a los demás requisitos mencionados en las secciones anteriores, pretenden resolver la cuestión del cuando verdaderamente existe o no consentimiento.

Como se analizó, en Europa el estándar es bastante claro y no está abierto a muchas interpretaciones. De hecho, ese es el objetivo principal de tener una normativa regional, la unificación legal en esta materia. De esta manera, es comprensible que el régimen jurídico más antiguo sea el más detallado, debido a que las discusiones sobre la protección de datos se han dado desde hace más de 20 años. También, es importante recalcar que la ayuda e influencia que tuvo el régimen europeo fue el plantear pautas importantes relativas a los principios rectores y los derechos inherentes de la protección de datos. Como se analizó, ellos fueron pioneros en reconocer un catálogo amplio e innovador de derechos de los titulares y de los que se encargan de recolectar los datos.

En este sentido, en Latinoamérica se aceptó esta herencia normativa y se la adaptó para cada situación en particular. Se estudio el ejemplo de Colombia, Perú y Ecuador siendo estos los países más innovadores en distintas situaciones. Colombia, por ejemplo, no trata al consentimiento como tal sino como una autorización del titular por lo que plantea menos requisitos, pero su estándar es igual de rígido. Perú en cambio, innovo con un reglamento integral el cual expande de manera clara y muy precisa conceptos planteados en la ley. En el caso del consentimiento, elabora de manera extensa los 5 requisitos que se enumeran en la ley. Finalmente, el ordenamiento ecuatoriano estableció su propio sistema conociendo los estudiados en este trabajo. Es decir, la importancia de estudiar ordenamientos ajenos al ecuatoriano radica en conocer cuál fue la inspiración que este recibió para su creación.

El caso ecuatoriano en cambio es poco usual. La LOPD personales obtuvo influencia de todos los cuerpos normativos estudiados, en específico del europeo. No obstante, esta ley carece de explicaciones claras de conceptos básicos de la materia. Específicamente, las explicaciones que hay del consentimiento son muy breves y algo ambiguas. Por lo que, como se mencionó en la sección anterior, resultaría muy positivo que un posible reglamento a la LOPD trate y desarrolle estos conceptos de manera preventiva a cualquier posible complicación. El tema intrigante es que el proyecto de ley presentado a la Asamblea sí contenía una explicación más elaborada de estos temas. Incluso, planteaban 2 requisitos innovadores para la manifestación del consentimiento. Además, permitía el trato de datos sensibles, pero con una rigidez en el consentimiento mucho más grande, estableciendo así, un sistema de manifestación del consentimiento positivo para la realidad ecuatoriana.

El fin principal de la normativa es proteger derechos de los titulares. En principio, el derecho a la autodeterminación informativa del cual se desprenden otros como el derecho a la privacidad, a la libertad personal, entre otros. Además, la normativa pretende establecer un ambiente amigable para las entidades recolectoras de los datos y así evitar posibles sanciones. La norma ecuatoriana trata de cumplir estos objetivos estableciendo artículos que faciliten y permitan un correcto tratamiento de los datos. Del mismo modo, en los casos de legislación extranjera se plantean herramientas como estándares estrictos, multas por incumplimiento y beneficios por cumplimientos para que la normativa aplicable resulte eficaz. No obstante, no es un trabajo solo del legislador o de la ley como tal, para que la ley resulte eficaz los intervinientes en situaciones negociales con objeto de protección de datos son los encargados de cumplir la norma por su propia convicción y de esta manera respetar el consentimiento del titular.