Universitat Oberta de Catalunya

uoc.edu

La regulación de la protección de datos personales en la legislación ecuatoriana y su análisis comparativo con el RGPD

Nombre Estudiante: Edison Pérez Vaca
Plan de Estudios del Estudiante: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del trabajo final: Aspectos legales de la seguridad informática

Nombre Consultor/a: Josep Cañabate Pérez
Nombre Profesor/a responsable de la asignatura: Montse Serra Vizern

Fecha Entrega: 31 de diciembre de 2020

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*La regulación de la protección de datos personales en la legislación ecuatoriana y su análisis comparativo con el RGPD*
Nombre del autor:	*Edison Pérez Vaca*
Nombre del consultor/a:	*Josep Cañabate Pérez*
Nombre del PRA:	*Montse Serra Vizern*
Fecha de entrega (mm/aaaa):	12/2020
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Aspectos legales de la seguridad informática*
Idioma del trabajo:	*Español*
Palabras clave	*RGPD, protección datos, Ecuador*

Resumen del Trabajo

La protección de datos personales es uno de los aspectos más importantes de la seguridad de la información, porque defiende un derecho de las personas. Varios países del mundo han desarrollado su legislación, con base al Reglamento general de protección de datos (UE) 2016/679. Sin embargo, en Ecuador se encuentra pendiente el análisis, debate y promulgación del Proyecto de Ley de Protección de Datos Personales.

El proyecto de Ley debe ser contrastado, con los aspectos generales y específicos del RGPD, para que se adapten a la realidad del Ecuador y de Latinoamérica, considerando las diferencias en aspectos: organizativos, comerciales, tecnológicos e incluso culturales.

El presente trabajo consiste en un análisis comparativo de los artículos del RGPD con los del proyecto de ley de Ecuador, y tiene como objetivo ser un insumo de análisis para la Asamblea Nacional, para este fin se presenta propuestas sustentadas de: modificación, adición o eliminación de varios artículos.

Los resultados indican que la mayoría de los artículos tienen semejanza con la estructura del RGPD: principios, derechos, figuras de responsabilidad, medidas de seguridad, transferencia de datos, autoridades de control y sanciones; sin embargo, también se ha encontrado diferencias importantes en la esencia de varios aspectos como: categorías de datos especiales, responsabilidad del encargado, independencia efectiva de la autoridad de control, definición de infracciones y estimación de sanciones, y consideraciones exclusivas para los servidores públicos. Diferencias que provocarían problemas en la aplicación efectiva de la ley, y en consecuencia una limitada defensa de los derechos de las personas.

Abstract:

The protection of personal data is one of the most important aspects of information security, because it defends a right of people. Several countries in the world have developed their legislation, based on the General Data Protection Regulation (EU) 2016/679. However, in Ecuador the analysis, debate and enactment of the Personal Data Protection Law Project is pending.

The bill must be contrasted, with the general and specific aspects of the RGPD, so that they adapt to the reality of Ecuador and Latin America, considering the differences in aspects: organizational, commercial, technological, and even cultural.

The present work consists of a comparative analysis of the articles of the RGPD with those of the Ecuadorian bill, and its objective is to be an input for analysis for the National Assembly, and for this purpose it presents supported proposals of: modification, addition or removal of multiple items.

The results indicate that most of the articles have similarities with the structure of the RGPD: principles, rights, figures of responsibility, security measures, data transfer, control authorities and sanctions; However, important differences have been found in the essence of aspects such as: special data categories, responsibility of the person in charge, effective independence of the control authority, definition of infractions and estimation of penalties, and exclusive considerations for public servants. Differences that could cause problems in the effective application of the law, and consequently a limited defense of people's rights.

Índice

1. Introducción

1.1. Contexto y justificación del trabajo

Los datos de cualquier índole constituyen el componente fundamental para construir la información. El conocimiento de la información representa un poder para el ser humano que la posea. Este es el motivo fundamental por el cual en la historia de la humanidad se ha dado radical importancia al manejo de los datos y la información. Con la revolución tecnológica en la que el mundo globalizado se desarrolla en la actualidad, el acceso a los datos personales ha cobrado una esencial relevancia, por cualquier motivo con el que se traten dichos datos, por ejemplo: para el desarrollo comercial o para la administración de los gobiernos, en la lucha contra: el crimen organizado, el terrorismo, la corrupción, los problemas de salud, etc.

El incremento en los últimos años del volumen de los datos personales recabados y su cada vez más sofisticado tratamiento ha concluido en la denominada "vigilancia masiva" [7]. Aunque menos antiguo en la historia, el debate sobre la aplicación efectiva al derecho a la privacidad de las personas, es decir el derecho a "no ser vigilado sin consentimiento" ha sido el punto de partida para el desarrollo normativo a nivel mundial de: leyes, reglamentos, normas, directivas que han pretendido garantizar dicho derecho, ahora conocido como la protección de los datos personales.

Así el 27 de abril de 2016, el Parlamento Europeo y el Consejo de La Unión Europea, adoptó el Reglamento (UE) 2016/679 (en adelante RGPD), 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. El RGPD fue el producto de varios años de debate, y como consta en los ciento setenta y tres (173) "considerandos", es el resultado de un profundo análisis de la convergencia y equilibrio de varios aspectos inherentes a la actualidad en la vida humana: derechos y libertades, desarrollo social y económico, seguridad jurídica, entre otros; y, a su vez, es la consecuencia de esperar décadas de la aplicación de leyes divergentes, adoptadas en los países miembros a partir de la Directiva de Protección de Datos (DPD - 1995), las que por la complejidad del tema, llegaron en su momento a dificultar el comercio y flujo libre de datos, porque chocaron en asuntos de "detalles" [8].

A partir del inicio de su aplicación e implementación, el 25 de mayo de 2018, el RGPD no repercutió únicamente en Europa, sino también en el mundo globalizado, que por el flujo de información y datos requeridos para cualquier transacción comercial, y con base al reconocimiento internacional de la alta calidad de la normativa europea, ha influenciado en la promulgación de leyes que lo tienen como la principal referencia. Los datos de Naciones Unidas[2], indican que un total de 107 países alrededor del mundo, lo que supone el 58%, cuentan ya con legislación sobre protección de datos o privacidad. Además, un 10% de los países cuenta con borradores de legislación y en otro 21% no hay legislación en la materia.

Por ejemplo en América Latina, en países como Brasil que no disponía de normativa previa específica, se emitió la ley para la protección de datos personales; y en otros países, como: Chile, Colombia, México y Perú, se pretende modificar su normativa interna para fortalecer este aspecto de la seguridad humana y adaptarla a las disposiciones del RGPD [9]. Incluso Argentina y Uruguay constan como países que brindan las garantías adecuadas en la protección de datos personales, para que los países de la Unión Europea puedan realizar transferencias internacionales [10].

Sin embargo, en la misma región, Ecuador es uno de los países que no cuenta con una regulación establecida para la protección integral de los datos personales ni con una Autoridad de Control. Convertido en un secreto a voces, el hecho que los datos personales de todos los ecuatorianos han sido y son utilizados desde hace varios años, para el establecimiento de llamadas, mensajes, correos electrónicos y cualquier forma de comunicación que permita la venta, publicidad o contacto comercial, y desde luego el uso de los datos para perpetrar fraudes informáticos, tuvo su consecuencia final en septiembre de 2019, cuando una empresa privada de seguridad informática publicó internacionalmente la noticia de que los datos de millones de habitantes estaban ubicados en un servidor no seguro de Miami – Estados Unidos, disponibles para la venta al mejor postor. Ante la evidencia internacional, el Gobierno Nacional de Ecuador apresuró la elaboración de un Proyecto de Ley de Protección de Datos Personales (en adelante Proyecto de Ley) que, en el mismo mes del incidente de seguridad, fue remitido a la Asamblea Nacional para su análisis y trámite pertinente, trámite que hasta la presente fecha no se inicia [1].

Si bien en Ecuador, existe una necesidad urgente e imperiosa de una regulación, no es menos cierto, que en cualquier enfoque legislativo debe considerarse la importancia de los datos personales para poder avanzar en materia de progreso social y desarrollo económico; la certidumbre y flexibilidad para las organizaciones que, con independencia de cuál sea su tipo o tamaño, tratan datos personales; y la protección efectiva de la persona física sin dejar de lado la interrelación de este derecho con otros, así como con la innovación tecnológica. En tal virtud, el documento de Ley que sea analizado y aprobado debe ser detenidamente contrastado, con los aspectos generales y específicos del RGPD, para que se adapten con la realidad del Ecuador y de Latinoamérica, sin descuidar las enormes fortalezas de la referencia europea, pero considerando las diferencias sustanciales en aspectos: organizativos, comerciales, tecnológicos, e incluso culturales.

El presente trabajo consiste en un análisis comparativo del RGPD con los artículos constantes en el nuevo Proyecto de Ley del Ecuador, y tiene como objetivo ser un insumo de análisis para la Asamblea Nacional, para lo cual se presentan propuestas sustentadas de modificación, adición o eliminación a varios artículos que se detallan a continuación.

1.2 Objetivos del Trabajo

- Determinar un estado de la situación actual de la protección de datos personales en el Ecuador.
- Establecer en qué medida el proyecto de ley de protección de datos personales en el Ecuador se alinea a lo establecido en el Reglamento (UE) 2016/679.
- Encontrar cuáles y de qué tipo son las diferencias entre el articulado del RGPD y el proyecto de ley.
- Elaborar propuestas específicas de modificaciones a cada artículo del proyecto de ley, para que se adapte a los objetivos del RGPD y se considere la realidad ecuatoriana.

1.3 Enfoque y método seguido

La metodología seguida es una investigación cualitativa, en la que a través de la observación se describen, comparan y analizan de forma minuciosa cada uno de los artículos del RGPD y del proyecto de ley.

Para la presentación del presente trabajo se asignan tres tipos de formato de texto y sombreado:

- tipo book para cada artículo del RGPD;
- tipo garamond para el artículo relacionado del Proyecto de Ley;
- tipo arial para el análisis personal del autor; y,
- tipo arial para el texto que contiene la propuesta de modificación, adición o eliminación del artículo. Adicionalmente, éstas propuestas se resaltan con cursiva el texto específico que se sugiere modificar.

El orden de los capítulos, secciones y artículos establecido en el RGPD se mantiene en el análisis comparativo, por tanto, la estructura de los artículos del Proyecto de Ley se adaptan a la estructura del RGPD.

1.4 Planificación del Trabajo

A continuación se presenta la planificación que se ha seguido durante la elaboración del presente trabajo:

No.	**Actividad**	**Número de semanas**												
		5-11 oct	**12-18 oct**	**19-25 oct**	**26-1 nov**	**2-8 nov**	**9-15 nov**	**16-22 nov**	**23-29 nov**	**30-6 dic**	**7-13 dic**	**14-20 dic**	**21-27 dic**	**28-1 ene**
		1	2	3	4	5	6	7	8	9	10	11	12	13
1	Búsqueda y selección de la información.	X	X											
2	Elaboración de registros de la bibliografía con síntesis del contenido.			X	X									
3	Presentación de documento con las fuentes de información y registros de la bibliografía consultada, con un resumen del contenido de cada uno de los registros.					X								
5	Elaboración de índice completo de la memoria						X							
6	Elaboración de borrador						X	X	X	X				
7	Presentación de documento con Índice y borrador del trabajo										X			
8	Revisión final											X	X	
9	Presentación del documento relativo a la memoria terminada y corregida.													X

1.5 Breve sumario de productos obtenidos

En el desarrollo del presente trabajo se han obtenido los siguientes productos:

- Estado de la situación actual de la protección de datos personales en el Ecuador.
- Diferencias entre el articulado del RGP y el proyecto de ley.
- Nivel de medida en que el proyecto de ley de protección de datos personales en el Ecuador se alinea a lo establecido en el Reglamento (UE) 2016/679.
- Propuestas de modificaciones al proyecto de ley, para que se adapte a los objetivos del RGPD y considerando la realidad ecuatoriana.

1.6 Breve descripción de los capítulos

En el capítulo 2 titulado el Estado de la cuestión, se presenta una recopilación de los principales artículos encontrados en las principales normas jurídicas del Ecuador, que tendrían como objetivo, en su ámbito, proteger el derecho de la protección de datos personales.

Con el capítulo 3 se inicia el análisis comparativo entre el RGPD y el Proyecto de Ley ecuatoriano, en dicho capítulo titulado Disposiciones Generales, se examinan los artículos relacionados con el objeto, el ámbito de aplicación y las definiciones.

El capítulo 4 presenta un estudio contrastado de los artículos referidos a los principios, el consentimiento y el tratamiento de tipo específico de datos personales.

En el capítulo 5 se revisan todos los derechos que asisten a los titulares (interesados) y que son derivados de la protección de datos personales, así como las limitaciones que se deben considerar para el ejercicio de los mismos.

El capítulo 6 hace mención a las figuras en materia de protección de datos personales, el responsable, el encargado y el delegado, se analizan sus obligaciones y las condiciones específicas en el tratamiento de datos.

Con el capítulo 7 denominado: Seguridad de los datos personales, se comparan los artículos que definen las obligaciones de los involucrados respecto a las medidas técnicas de seguridad que deben implantarse en el tratamiento de los datos, las obligaciones derivadas de estas medidas, que pueden incluir procesos de certificación acerca de la adopción de las normas de seguridad.

En el capítulo 8 titulado Transferencias internacionales, se estudia de forma comparada los aspectos que posibilitan a los responsables del tratamiento realizar transferencia de datos personales a destinatarios internacionales.

En el capítulo 9 titulado Autoridad de Control, se examinan el principio de independencia y las condiciones generales para el Organismo y su autoridad en materia de protección de datos personales.

El capítulo 10 denominado Recursos, responsabilidades y sanciones, se describen los artículos que otorgan a los interesados derechos adicionales ante el incumplimiento de las normas establecidas. De esta forma se determinan la clasificación de las infracciones y las eventuales sanciones que podrían imponerse.

Finalmente en el capítulo 11, se revisan las disposiciones finales del Proyecto de ley.

2. Estado de la cuestión

El estado de la cuestión en materia de protección de datos personales en Ecuador refleja que existen varios artículos relacionados con la privacidad, confidencialidad o protección de datos personales, redactados en varios cuerpos legales, reglamentarios y normativos [11]. A continuación se describen los de mayor relevancia:

Constitución de la República del Ecuador:

Artículo 40. (Movilidad Humana)
(…)
5. Mantendrá la **confidencialidad** de los datos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior.

Artículo 66. (Derechos de libertad)
El derecho a la **intimidad** personal y familiar.

Artículo 92. (Acción de hábeas data)
Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de **datos personales** e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

Artículo 362. (Salud)
(…). Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la **confidencialidad** de la información de los pacientes.

Artículo 329. (Formas de trabajo y su retribución)
(…) Los procesos de selección, contratación y promoción laboral se basarán en requisitos de habilidades, destrezas, formación, méritos y capacidades. Se prohíbe el uso de criterios e instrumentos discriminatorios que afecten la **privacidad**, la dignidad e integridad de las personas.

Ley Orgánica de garantías jurisdiccionales y control constitucional:

Artículo 49 Objeto.
La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sé misma, o sobre sus bienes, están en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.
El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los

datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.
Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos:

Definición Intimidad.- El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Artículo 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Artículo 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta Ley.

Reglamento a la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos:

Artículo 21.
(…)
Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta Ley.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos:

Artículo 5.- Publicidad.- El Estado, de conformidad con la Ley, pondrá en conocimiento de las ciudadanas o ciudadanos, la existencia de registros o bases de **datos de personas** y bienes y en lo aplicable, la celebración de actos sobre los mismos, con la finalidad de que las interesadas o interesados y terceras o terceros conozcan de dicha existencia y los impugnen en caso de afectar a sus derechos.

Artículo 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, sólo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.
Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de Identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer. La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad.

Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos:

Artículo 11.- Principios para el tratamiento de datos personales.- Todo tratamiento de datos públicos que se haga por parte de la Dirección Nacional de Registro de Datos Públicos, de las instituciones que componen el Sistema Nacional de Registro de Datos Públicos, y en general, por las personas naturales o jurídicas, públicas o privadas, que mantuvieren o administren por disposición legal información registral de carácter público, deberá observar los siguientes principios: (…)

Artículo 12.- Rectificación, actualización, eliminación y anulación de datos.- Sin perjuicio de las demás acciones previstas en el ordenamiento jurídico, toda rectificación, actualización o eliminación de los datos que consten en los registros públicos únicamente podrá ser solicitada por el titular de los mismos, quien deberá presentar los documentos que justifiquen la modificación exigida. La solicitud deberá presentarse directamente a la entidad de la que provenga el dato cuyo cambio se exige. (…)

Disposición General Séptima.- Para los fines del presente Reglamento, se establecen las siguientes definiciones:
2. Datos accesibles.- (…)
3. Datos confidenciales.- (…)
4. Datos públicos.- (…)
5. Entes Registrales.- (…)
8. Información pública.- (…)
10. Protección de Datos.- (…)
11. Responsable del tratamiento de datos.- (…)
12. Tratamiento de datos.- (…)”

Ley Orgánica de Telecomunicaciones:

Artículo 78.- Derecho a la intimidad.
Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. (…)

Artículo 79.- Deber de información.
(…) En caso de violación de los datos de un abonado o usuario particular, el prestador notificará de tal violación al abonado o usuario particular en forma inmediata, describiendo al menos la naturaleza de la **violación de los datos personales**, los puntos de contacto donde puede obtenerse más información, las medidas recomendadas para atenuar los posibles efectos adversos de dicha violación y las medidas ya adoptadas frente a la violación de los datos personales.
La notificación de una violación de los datos personales a un abonado, cliente o usuario particular afectado no será necesaria si el prestador demuestra a la Agencia de Regulación y Control de las Telecomunicaciones que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.
A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicio de telecomunicaciones.

Artículo 80.- Procedimientos de revelación.
Las y los prestadores de servicios implementarán procedimientos internos para atender las solicitudes de acceso a los datos personales de sus abonados, clientes o usuarios por parte de las autoridades legalmente autorizadas. Los procedimientos internos que se implementen, para fines de supervisión y control, estarán a disposición de la Agencia de Regulación y Control de las Telecomunicaciones.

Artículo 81.- Guías telefónicas o de abonados en general.
Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados. Deberán ser informados de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías.

Artículo 82.- Uso comercial de datos personales.
Las y los prestadores de servicios no podrán usar **datos personales**, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento previo y expreso. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico.
Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personales de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados

Artículo 83. Control técnico.
(…) Cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las

comunicaciones y **seguridad de datos personales**, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la seguridad e integridad de las redes, la Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.

Artículo 84.- Entrega de información.
Las y los prestadores de servicios, entregarán a las autoridades competentes la información que les sea requerida dentro del debido proceso, con el fin de investigación de delitos. La Agencia de Regulación y Control de las Telecomunicaciones establecerá los mecanismos y procedimientos que sean necesarios.

Artículo 85.- Obligaciones adicionales.
(…) La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de **seguridad de datos personales** y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios.

Reglamento a la Ley Orgánica de Telecomunicaciones:

Artículo 120. Garantía de protección de datos personales.-
Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, esto es, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la LOT, su Reglamento General y las regulaciones emitidas por la ARCOTEL para el efecto. La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico.

Artículo 121. Uso comercial.- Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo autorización y consentimiento expreso del usuario.
Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento expreso, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. En dicho instrumento se deberá dejar constancia expresa de los datos personales o información que están expresamente autorizados; el plazo de la autorización y el objetivo que esta utilización persigue. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías.
La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de los datos personales y de las redes

Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación:

Artículo 67.- Ética en la investigación científica
(…)
5.- Confidencialidad de los datos personales, así como aquellos exceptuados en el Código de Ética Nacional obtenidos en procesos de investigación;

Resolución No. SB-2017-810 de la Superintendencia de Bancos:

Artículo 14.- (Derecho a protección)
El usuario tendrá derecho a recibir protección y a demandar la adopción de medidas efectivas que garanticen la seguridad de las operaciones financieras, del defensor del cliente, de la Superintendencia de Bancos o de otras instancias administrativas o judiciales pertinentes, especialmente en los siguientes casos:
(…)
b. Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos o servicios financieros. La información sobre dichos datos personales solo podrá ser otorgada por la entidad de los sectores financieros público y privado, en caso de consentimiento libre y expreso, especifico, inequívoco e informado, por parte del usuario, de disposición judicial o del mandato de la ley; (…)

Código Orgánico General de Procesos COGEP:

Artículo 7.- Principio de intimidad.
Las y los juzgadores garantizarán que los datos personales de las partes procesales se destinen únicamente a la sustanciación del proceso y se registren o divulguen con el consentimiento libre, previo y expreso de su titular, salvo que el ordenamiento jurídico les imponga la obligación de incorporar dicha información con el objeto de cumplir una norma constitucionalmente legítima.

Artículo 8.- Transparencia y publicidad de los procesos judiciales.
La información de los procesos sometidos a la justicia es pública, así como las audiencias, las resoluciones judiciales y las decisiones administrativas. Únicamente se admitirá aquellas excepciones estrictamente necesarias para proteger la intimidad, el honor, el buen nombre o la seguridad de cualquier persona.

Código Orgánico Monetario Y Financiero, Libro I:

Artículo 357.- Registro de Datos Crediticios.
El servicio de referencias crediticias será prestado por la Superintendencia de Bancos y por las personas jurídicas autorizadas por la Superintendencia de Bancos, entidad que está facultada para supervisar y controlar el ejercicio de sus actividades.

Artículo 360.- Protección de la información.
Las personas que por diversas causas lleguen a tener acceso a reportes emitidos por la Superintendencia de Bancos respecto del Registro de Datos Crediticios deberán obligatoriamente guardar confidencialidad sobre la información contenida en ellos, siendo prohibido utilizarla para fines distintos del análisis crediticio.

Se prohíbe a toda persona natural o jurídica la comercialización, por cualquier medio, de la información de referencias crediticias. Quien contravenga lo dispuesto en esta disposición, empleare o divulgare indebidamente la información contenida en un reporte de crédito y/o alterare la información proporcionada por la fuente, estará sujeto a las sanciones establecidas en la legislación vigente, sin perjuicio de las acciones y responsabilidades administrativas, civiles y penales a las que hubiere lugar.
La información que consta en los reportes crediticios incluirá la identidad de todas las personas o entidades que obtuvieron un reporte o accedieron a una consulta del historial crediticio del titular, así como la fecha en que se emitieron tales reportes o consultas.
El acceso a la información del Registro de Datos Crediticios, no tendrá restricciones para el titular de la misma; sin embargo, en el caso de terceros debidamente autorizados únicamente podrá ser consultada la información de las operaciones de los tres (3) últimos años. Los servidores del Registro de Datos Crediticios que tengan acceso a la información deberán guardar la correspondiente reserva y sigilo.
El titular de la información crediticia tiene derecho a exigir la fuente de la información crediticia. La rectificación de la información ilegal, inexacta o errónea se comunicará al organismo de control pertinente, que a su vez comunicará a la Superintendencia de Bancos para la actualización del Registro de Datos Crediticios. Si se concluye que la información materia de impugnación del titular es ilegal, inexacta o errónea, el Registro de Datos Crediticios, por cuenta de la fuente de información crediticia, inmediatamente enviará comunicaciones rectificatorias a todos quienes hubieren recibido reportes conteniéndola.
Las fuentes de información crediticia serán legalmente responsables por los daños ocasionados al titular como consecuencia de la transmisión de información ilegal, inexacta o errónea que afecten su calificación o historial de crédito y, por tanto, no estarán exonerados alegando ausencia de dolo o de culpa.

2.1. Situación actual

En Ecuador, en materia de protección de datos personales, con términos a referidos: intimidad, confidencialidad, privacidad, habeas data, acceso, rectificación y transparencia de información, existen aproximadamente 5 artículos constitucionales, 14 artículos legales, 6 artículos reglamentarios, 6 artículos codificados y 1 artículo resolutivo. Un total aproximado de 31 artículos dispuestos en cuerpos normativos de diferentes sectores: judicial, financiero, sanitario, telecomunicaciones, comercio electrónico y registro público. Esta dispersión denominada “normativa especializada”, no brinda un marco legal sólido y estructurado que garantice el ejercicio de este derecho fundamental consagrado en la Constitución.

Aunque se establece el derecho a la protección de datos personales, esta protección por sí sola es insuficiente por los siguientes motivos [21]:
- Es general, porque deja muchos campos abiertos para la interpretación.
- No existen reglas claras sobre el manejo de datos personales.
- No está enfocada en un medio transnacional como el internet.
- No establece una autoridad de protección de datos

En los siguientes capítulos se desarrollará el análisis objeto del presente trabajo.

3. Disposiciones generales

3.1. Objeto

Artículo 1. Objeto
1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 1. Objeto
El objeto de la presente Ley es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digítales en el tratamiento y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela.

La futura Ley de Protección de Datos Personales de Ecuador requerirá la expedición posterior de un Reglamento General, que desarrolle la aplicación de la misma; en tal sentido, el término "regular el ejercicio de los derechos establecidos en la ley" debería ser utilizado en el objeto del futuro Reglamento. En su lugar, la Ley debería utilizar la frase "proteger los derechos".

En lo que se refiere al derecho a la protección de datos, éste no es un derecho absoluto o ilimitado, y tiene sus límites en la medida de proteger también otros derechos (libertad de expresión, propiedad intelectual, salud pública, etc.). Por esto, se requiere establecer de forma expresa a quien pertenece el derecho, tal como lo especifica el RGPD: "el derecho de las personas físicas."

En otros países como Argentina, en el proceso de formación de la ley nacional de protección de datos en el año 2001 se expidió la Ley 25.326, la cual extiende el derecho a la protección de los datos personales, a las personas jurídicas. Sin embargo el criterio y la experiencia argentina señalan que esta extensión puede ser peligrosa para el estado de derecho, porque puede hacer oscura la actividad de las personas jurídicas, contradiciendo los principios de transparencia y legalidad. Otros países como Chile y España no consideraron dicha extensión [19].

El término autodeterminación informativa, que es la atribución que tiene el titular de conocer y consentir sobre el uso de sus datos personales [12], no se incluye en la sección "Definiciones", por esto no se debería incluir en el texto del objeto. Por otra parte, el enunciado "*a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela*", se refiere a las formas en que establecería las normas para conseguir el objeto de la Ley, pero ésta formas no constituyen el objeto.

Propuesta Nro.1: Modificar Artículo 1. Objeto.

El objeto de la presente Ley es *proteger los derechos de las personas físicas, relativos a la protección de los datos personales; y, garantizar los demás derechos digítales en el tratamiento y flujo de estos datos*.

Artículo existente únicamente en el Proyecto de Ley:

Artículo 2. Finalidad: La finalidad de la presente Ley es procurar el adecuado tratamiento y flujo de datos personales para garantizar los derechos fundamentales y las libertades individuales, promover el progreso económico y social; impulsar la producción nacional y la cooperación internacional; fomentar la competitividad, la innovación y productividad, elevar la eficiencia de los servicios públicos y/o privados; y, mejorar la calidad de vida.

Dicha redacción es similar al objeto de la Ley. La Ley de Protección de Datos Personales no pertenece al sector económico o social, no se considera oportuno establecer una finalidad relacionada con la producción, competitividad, innovación y productividad, esto podría incluirse en los considerandos, más no en la finalidad porque se puede opacar el verdadero objeto de la Ley.

Propuesta Nro. 2: Eliminar.- Articulo 2. Finalidad

3.2. Ámbito de aplicación material

Aplicación:

Artículo 2. Ámbito de aplicación material
1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. (…)

Artículo 3. Ámbito de aplicación material
La presente Ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, ya sean totalmente automatizados, parcialmente automatizados o no automatizados y a toda modalidad de uso posterior, por parte de responsables o encargados del tratamiento de datos personales. (…)

En el Proyecto de Ley se menciona a los datos contenidos en cualquier tipo de soporte y con tipo de tratamiento: automatizado, parcialmente automatizado o no automatizado. Sin embargo, los términos del RGPD no emplea en su redacción, la expresión “a cualquier tratamiento” [5] y distingue dos casos:

- tratamiento total o parcialmente automatizado,
- tratamiento no automatizado contenidos o destinados a ser incluidos en un fichero.

Se distingue la diferencia respecto al tratamiento no automatizado: en el Proyecto de Ley, en cualquier tipo de soporte; y en el RGPD, de datos destinados a un fichero.
El Proyecto carece de dos definiciones: del término “soporte” y del término “fichero” (que se menciona en la consideración de la página 11 y en el numeral 5 del artículo 48). Por otra parte, aunque en el RGPD sí define en el artículo 4 el término fichero, se suprime esta expresión y la reemplaza por la palabra “tratamiento”. Ya no se habla de “ficheros de datos personales”, sino de “tratamientos de datos personales” [3].

El Proyecto de Ley tal como se encuentra redactado en su artículo 3 y sin definir los términos mencionados, abre dos posibilidades:

a) Que el elemento que contiene los datos no sea considerado soporte y se lo excluya aunque se pueda acceder a los datos; o,
b) Que existan datos en soportes pero que no permitan el acceso y a pesar de eso se los incluya por el hecho de estar contenidos en un soporte.

Por tanto, en el Proyecto de Ley no es necesario definir fichero (a la par con la eliminación de esta expresión en el RGPD), pero sí es necesario agregar esta aclaración: que se refiere a cualquier tipo de soporte siempre que permita su utilización, almacenamiento, organización y acceso [3].

Respecto al término *"a toda modalidad de uso posterior*", el proyecto podría caer en una indeterminación con la frase "uso posterior", por lo que debería definir cuáles son los usos posteriores: utilización, almacenamiento, organización y acceso.

Propuesta Nro. 3: Modificar Articulo 3. Ámbito de aplicación material

La presente Ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte *que permita su utilización, almacenamiento, organización y acceso; ya sean totalmente automatizados, parcialmente automatizados o no automatizados*, por parte de responsables o encargados del tratamiento de datos personales.

No Aplicación:

Artículo 2. Ámbito de aplicación material (*Continuación*)
2. El presente Reglamento no se aplica al tratamiento de datos personales:
a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
3. El Reglamento (CE) n.o 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.o 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.
4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. Ámbito de aplicación material (*Continuación*)
La presente ley no será aplicable a:
1. El tratamiento de datos personales utilizados en actividades familiares o domésticas;
2. Datos anónimos, y,
3. Datos que identifican o hacen identificable a personas jurídicas
Son accesibles al público y susceptibles de tratamiento los datos personales de contacto de comerciantes; representantes y socios de personas jurídicas; así como los de servidores

públicos siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo.
El histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos, por la naturaleza de su cargo, se considerará accesible al público y susceptible de tratamiento.

La intención del Proyecto es agregar tres tipos de datos adicionales para los cuales no es aplicable la ley:

- Datos de contacto de comerciantes cuando se refieran al ejercicio de su profesión, oficio, giro de negocio,
- Datos de contacto de representantes y socios de personas jurídicas cuando se refieran al giro de negocio,
- Datos de servidores públicos cuando se refieran a sus competencias, facultades, atribuciones o cargo. El histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos.

El mismo Proyecto de Ley incluye posteriormente exclusiones a su aplicación. Sin embargo, definir que ciertos grupos de datos no se contemplan en el ámbito de aplicación material, puede interpretarse como la creación de una categoría diferenciada de datos, como si los comerciantes, socios de personas jurídicas y servidores públicos no fueran personas físicas y que aun cuando los identifiquen no son datos personales, lo cual contradice notoriamente la definición. Es posible que las motivaciones para tal redacción del artículo sean las siguientes:

- Datos de comerciantes: facilitar el intercambio comercial.
- Datos de socios de personas jurídicas y de servidores públicos: el combate a la corrupción.

Para la finalidad de facilitar el intercambio comercial (a la par del RGPD que establece las bases para el libre intercambio comercial dentro de la UE), es posible indicar que no es necesario para las actividades comerciales registrar las agendas de las bases de datos comerciales ante la Autoridad de control.

Para la finalidad de combate a la corrupción, existen leyes y procedimientos que obligan a dichas personas naturales a dar su consentimiento de tratamiento de sus datos para realizar su negocio o para asumir un cargo público. Además con el debido proceso judicial se pueden emitir órdenes que legitimen el tratamiento de los datos aun sin recibir el consentimiento del interesado.

En definitiva los datos de comerciantes, socios de empresas y servidores públicos, si constituyen datos personales y deberían ser protegidos en la Ley de Protección de Datos Personales, sin perjuicio que a través de otras normas, según corresponda, sean tratadas sin el consentimiento del titular porque en ese caso, como se analizará más adelante, la base de la legitimidad es el interés público.

En este sentido, en el territorio español, la Ley Orgánica 3/2018 (Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales, en adelante LOPDGDD), en su artículo 19, establece la protección frente al tratamiento de los datos de contacto relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a. Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.
b. Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

Como se observa no existe la posibilidad de libre tratamiento de los datos personales de contacto únicamente por referirse al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo; sino que también, se requiere que la finalidad del tratamiento sea únicamente mantener relaciones con la persona jurídica en la que preste sus servicios, es decir, que no se traten para entablar una relación con los mismos como personas físicas [3].

Propuesta Nro. 4: Articulo 3. Ámbito de aplicación material

Cambiar: Datos anónimos por Datos anonimizados

Agregar: Datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 42

Modificar el párrafo a partir del apartado número 3:

Son accesibles al público y susceptibles de tratamiento los datos personales de contacto de comerciantes; representantes y socios de personas jurídicas; así como los de servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo; *y, la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios, es decir que no se traten para entablar una relación con los mismos como personas físicas.*

3.3. Ámbito de aplicación territorial

Artículo 3. Ámbito territorial
1. El presente Reglamento se aplica al 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.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o no
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.
3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. Ámbito de aplicación territorial.
Se aplicará la presente Ley cuando:
1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional;
2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;

3. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y oferte bienes o servicios a personas localizadas en el territorio nacional, independientemente de si se requiere su pago o no,
4. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y realice actividades relativas a la recogida de datos personales de personas localizadas en el territorio nacional; y,
5. Al responsable o encargado del tratamiento de datos personales no domiciliado en el territorio nacional que le resulte aplicable la legislación nacional, en virtud de la celebración de un contrato o del derecho internacional público.

La aplicación territorial debe definir: ubicación del responsable, ubicación del interesado o titular y ubicación del tratamiento.

El apartado 1 del Proyecto de Ley define la ubicación del tratamiento, sin importar si el responsable o los interesados se encuentran en el territorio nacional. Se entrega importancia específica a la ubicación del equipo computacional utilizado para el tratamiento de los datos, sin embargo es necesario aclarar que el objeto de interés de la protección de datos personales debe referirse a los interesados ubicados en el país y no en cualquier parte del mundo.

El apartado 1 del RGPD define la ubicación del responsable sin importar el lugar del tratamiento, lo que es concordante con el apartado 2 del proyecto que define la ubicación nacional del responsable o encargado.

Los apartados 3 y 4 del Proyecto de Ley se refieren a la oferta de bienes y servicios, lo único que difiere es que el numeral 4 no define la finalidad de la recolección de datos. Es factible unificar los apartados 3 y 4.

Propuesta Nro. 5: Modificar.- Articulo 4. Ámbito de aplicación territorial.

1. El tratamiento de datos personales localizados en el territorio nacional se realice en cualquier parte del territorio nacional;
2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;
3. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y oferte bienes o servicios a personas localizadas en el territorio nacional, independientemente de si se requiere su pago o no; o, realice actividades relativas a la recogida de datos personales de personas localizadas en el territorio nacional; y,
4. Al responsable o encargado del tratamiento de datos personales no domiciliado en el territorio nacional que le resulte aplicable la legislación nacional, en virtud de la celebración de un contrato o del derecho internacional público.

3.4. Definiciones

En la siguiente tabla se compara las definiciones del RGPD y del Proyecto de Ley con una observación sobre la concordancia o no, de ser el caso:

RGPD **Artículo 4. Definiciones**	**Proyecto de Ley** **Artículo 5. Términos y definiciones**	**Observa_ción**
	Anonimización: La aplicación de medidas de cualquier naturaleza dirigidas a **Impedir la identificación** o re-identificación de una persona natural sin esfuerzos desproporcionados.	No existe en RGPD
5) «seudonimización»:el tratamiento de datos personales de manera tal que **ya no puedan atribuirse a un interesado sin utilizar información adicional**, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;		No existe en Proyecto de Ley
	Base de datos: Conjunto configurado, estructurado o no estructurado de datos, cualquiera que fuere la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento y acceso.	No existe en RGPD
11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, 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;	Consentimiento: Manifestación de voluntad libre, previa, especifica, expresa, informada e inequívoca, por la que el titular de los datos personales **autoriza al responsable** del tratamiento de datos personales a tratar los mismos.	
14)«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;	Dato biométrico: Dato personal único obtenido a partir de un tratamiento técnico-especifico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. **entre otro**	concordante
13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;	Dato genético: Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo: generalmente se analizan a partir de muestras biológicas.	concordante
1) «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	Dato personal: 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.	Análisis posterior

elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;		
	Datos personales crediticios: Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera.	No existe en RGP
	Datos personales registrables: Datos personales que conforme al ordenamiento jurídico deben estar contenidos en Registros Públicos	No existe en RGP
15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;	Datos sensibles: 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	Categoría especial de datos
9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento	Destinatario: Persona natural o jurídica que ha recibido comunicación de datos personales.	concordante
	Disociación de datos: Todo tratamiento de datos personales destinado a que éstos no puedan ser asociados o vinculados a una persona identificada o identificable.	
4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;	Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o patrones relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.	concordante

8) «encargado del tratamiento» o «encargado»: la **persona física o jurídica, autoridad pública, servicio u otro organismo** que trate datos personales por cuenta del responsable del tratamiento;	Encargado del tratamiento de datos personales: **Persona** que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.	Proyecto no especifica si es persona natural o jurídica, pública o privada
	Estado de la técnica: Estado último de cualquier **particularidad que permita establecer bases de comparación** para determinar si los requisitos o herramientas de carácter administrativo, físico, técnico, organizativo, jurídico u otros constituyen niveles adecuados de protección en el tratamiento de datos personales.	No existe en RGP
	Filtración: Es un Incidente Ilegal o no autorizado que involucra la visualización, acceso, extracción o divulgación de datos personales por un individuo, aplicación, servicio u otros.	Caso específico de una vulneración de seguridad
	Fuentes accesibles al público: Bases de datos que pueden ser consultadas por cualquier persona natural o Jurídica, pública o privada, nacional o internacional cuyo acceso no se encuentre limitado por la normativa vigente o disposición de la Autoridad de Protección de Datos Personales	No existe en RGP
	Política de tratamiento de datos personales: Documento físico, electrónico o en cualquier formato generado por el responsable del tratamiento de datos personales que debe obligatoriamente ponerse a disposición del titular, a partir del momento en el cual se recaben sus datos personales y debe estar disponible de forma permanente, con el objeto de garantizar el derecho a la transparencia, cuyo contenido será definido por la Autoridad de Protección de Datos Personales.	No existe en RGP
7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo **que, solo o junto con otros, determine los fines** y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;	Responsable del tratamiento de datos personales: Persona natural o jurídica, pública o privada, **que decide sobre la finalidad** y el tratamiento de datos personales	Concordante
	Sellos de Protección de Datos Personales: Acreditación que otorga la Entidad Certificadora al responsable o al encargado del tratamiento de datos personales, de haber Implementado mejores prácticas en sus procesos, con el objetivo de promover	No existe en definiciones RGP

	la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.	
10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado	Tercero: Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o. Autoridad de Protección de Datos Personales, conforme al alcance establecido en la presente Ley.	concordante
	Titular: Persona natural cuyos datos son objeto de tratamiento.	Concordante con interesado
	Transferencia o comunicación: Manifestación, declaración, publicación, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de **revelación de datos personales realizada a una persona distinta al titular**, responsable o encargado del tratamiento de datos personales. Los datos personales que han de comunicarse deben ser exactos, completos y actualizados.	No existe en definiciones RGP
2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;	Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, **eliminación, indexación**, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, comunicación por transmisión, transferencia, difusión, **procesamiento, almacenamiento, distribución, cesión**, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción **y, en general, cualquier uso de datos personales.**	Generalidad: "cualquier uso"
12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;	Vulneración de la seguridad de los datos personales: **Incidente de seguridad** que afecta la confidencialidad, disponibilidad o integridad de los datos personales, como por ejemplo la filtración.	No existe definición de incidente en Proyecto

Definición de datos personales

«**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.

Dato personal: 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

En el Proyecto de Ley existe una redundancia en la definición con la propia palabra definida (dato personal es un dato...). En el RGPD el uso de la frase "toda o cualquier información" implica que la naturaleza de la información es irrelevante y que cualquier información relativa a una persona física sería considerada como dato personal, de esta forma el RGPD pretende que el alcance de la normativa sea amplia y no limitada [4].

La frase: *"datos inocuos, metadatos o fragmentos de datos"* es desproporcionada, porque interpretar que una información siempre es un dato personal podría dar lugar a una aplicación desproporcionada de la ley, por esto el término "sobre" significa que el dato tiene que proporcionar información relativa a una persona física, que la identifica o la hace identificable. Da igual cual sea la forma, por ejemplo, alfabética, numérica, gráfica, fotográfica o sonora, así como el soporte, sea en papel o automatizado [4].

En Ecuador persona natural es sinónimo de persona física. De la misma manera titular de los datos personales a efectos de la Ley es sinónimo de interesado.
En el Proyecto de ley debe señalarse de forma clara y precisa los cuatro elementos del concepto de datos personales: "toda o cualquier información"; "sobre"; "una persona física"; e, "identificada o identificable".

Propuesta Nro. 6: Modificar.- Articulo 5. Definición de Dato Personal.

*Toda o cualquier información sobre una persona natural, que permite, directamente o indirectamente, indentificarla o hacerla indentificable mediante el uso de un identificador***.**

Definición de tratamiento

«**tratamiento**»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

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

La definición de tratamiento del proyecto de ley se basa en la definición del documento *"Estándares de Protección de Datos Personales para los Estados Iberoamericanos"* (20/06/2017), y es ampliamente coincidente con la definición del RGPD. No obstante en la del Proyecto de Ley, el término *"(…) en general, cualquier uso de datos personales"*, implica una aplicación muy extensa, que puede ser ilimitada y desproporcionada.

Propuesta Nro. 7: Modificar.- Articulo 5. Definición de Tratamiento.

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, comunicación por transmisión, transferencia, difusión, procesamiento, almacenamiento, distribución, cesión, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión y destrucción.

Definiciones de Seudonimización, Disociación, Anonimización.

En el RGPD se define la "seudonimización" como la técnica que consiste en sustituir un único atributo, de manera que las personas que tengan acceso a todos los datos todavía puedan identificar a las personas. Por eso, los datos seudonimizados siguen siendo datos personales.

Por otra parte el Proyecto de Ley no contempla la definición anterior, y en su defecto presenta las definiciones de:
"anonimización" como la técnica que elimina todos los identificadores únicos, por lo que, con un proceso irreversible, se impide identificar a la persona y por tanto, los datos anonimizados ya no son datos personales; y
"disociación de datos", que de la misma forma provoca que luego del tratamiento no se puede identificar a la persona, por lo que los datos disasociados ya no son datos personales.

En tal sentido, únicamente el tratamiento de los datos seudonimizados (que siguen siendo datos personales) se encuentra en el ámbito de aplicación de la protección de datos personales; los datos anonimizados no (porque ya no son datos personales).

Propuesta Nro. 8: Agregar al Artículo 5. Definición de seudonimización.

El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

Definiciones de transferencia y transmisión

Transferencia o comunicación: Manifestación, declaración, publicación, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que han de comunicarse deben ser exactos, completos y actualizados.

Los conceptos de transferencia (comunicación) y transmisión (remisión) son diferentes, por esta razón, se considera que existe un error en la definición anterior del Proyecto de Ley, porque combina los dos enunciados. En el caso de la comunicación o transferencia, un responsable comunica o transfiere los datos personales a otro u otros responsables del tratamiento de manera que estos últimos los tratarán para sus propias finalidades. En el caso de la remisión o transmisión, aunque materialmente hay también una cesión o envío, no se considera una "transferencia" ya que lo que se produce es el tratamiento de los datos personales por un encargado del tratamiento, con el objetivo de que el encargado preste un servicio al responsable, sin que el encargado defina sus propias finalidades.

Propuesta Nro. 9: Modificar.- Articulo 5. Definición de Transferencia o comunicación.

Manifestación, declaración, publicación, entrega, interconexión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales; *para que el destinatario de dicha transferencia realice un tratamiento de los datos personales para sus propias finalidades.*

Propuesta Nro. 10: Añadir.- Articulo 5. Definición de Transmisión o remisión.

Cesión o envío de datos personales al encargado del tratamiento, con el objetivo de que el encargado preste un servicio al responsable, que involucra el tratamiento de los datos personales enviados, *sin que el encargado tome ciertas decisiones fundamentales sobre el tratamiento.*

Términos definidos en el RGPD y no definidos en el Proyecto de Ley

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

En el artículo 32 del Proyecto de Ley, se establece una sección de la limitación del tratamiento, no se considera necesario añadir dicha definición.

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

Conforme el análisis anterior de la definición de datos personales, el término fichero no se considera necesario.

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.
18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;
19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas
20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio

de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;
26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Las definiciones anteriores se citan en el capítulo de transferencias internacionales.

16) «establecimiento principal»:
a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;
b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;
23) «tratamiento transfronterizo»: a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

Las definiciones anteriores tienen relación directa con el ámbito de aplicación territorial del RGPD, no se requieren en el Proyecto de Ley.

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;
22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control;

Las definiciones anteriores se incorporan en el Proyecto de Ley en el capítulo de la Autoridad de Protección de Datos Personales.

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el

encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;
25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (1);

Los términos anteriores no se incorporan en el Proyecto de Ley, por tanto no se requieren sus definiciones.

Artículo del Proyecto de Ley sin análogo en el RGPD

Artículo 6. Sujetos intervinientes: Son parte del sistema de protección de datos personales, lo siguientes sujetos:
1. Titular.
2. Responsable del tratamiento;
3. Encargado del tratamiento;
4. Tercero;
5. Destinatario;
6. Autoridad de protección de datos;
7. Entidades certificadoras; y.
8. Delegado de protección de datos personales.

Artículo 7. Normas aplicables al ejercicio de derechos: El ejercicio de los derechos a la protección de datos personales, se canalizará a través del responsable del tratamiento. Autoridad de Protección de Datos Personales y/o jueces competentes, de conformidad con el procedimiento establecido en la presente ley.

En el artículo 7 se establece más actores que en el artículo 6, "los jueces competentes", lo que resulta innecesario porque en todo el documento se establece la intervención de las órdenes judiciales como un elemento que puede intervenir en la aplicación efectiva de la ley.

Propuesta Nro. 11: Eliminar.- Articulo 7. Normas aplicables al ejercicio de derechos.

4. Principios

Los principios que se definan son muy importantes puesto que en caso de vacíos legales, éstos serán la guía para que el tratamiento de los datos sea conforme a la normativa [3]. Además en la sección del régimen sancionatorio el incumplimiento a los principios será considerado una infracción.

4.1. Principios relativos al tratamiento

Artículo 5. Principios relativos al tratamiento
1. Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 8. Principios
Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de juridicidad, lealtad y transparencia, legitimidad, finalidad, pertinencia y minimización de datos personales, proporcionalidad del tratamiento, consentimiento, confidencialidad, calidad, conservación, seguridad de datos personales; responsabilidad proactiva y demostrada, aplicación favorable al titular; e, independencia de control.

El Proyecto del Ley, presenta doce (12) principios, únicamente nueve (9) de los cuales tienen plena coincidencia con los expuestos en el RGPD, tal como se señala a continuación:

1. juridicidad, lealtad y transparencia, legitimidad; con el principio a) licitud, lealtad y transparencia
2. finalidad; con el principio b) limitación de la finalidad
3. pertinencia y minimización de datos personales; con el principio c) minimización de datos
4. proporcionalidad del tratamiento; con el principio c) minimización de datos
5. calidad; con el principio d) exactitud
6. conservación; con el principio e) limitación del plazo de conservación
7. confidencialidad; con el principio f) integridad y confidencialidad
8. seguridad de datos personales; con el principio f) integridad y confidencialidad
9. responsabilidad proactiva y demostrada; con el apartado 5.2 responsabilidad proactiva
10. consentimiento; sin concordancia
11. aplicación favorable al titular; sin concordancia

12. independencia de control; sin concordancia

En tal sentido existen tres principios del Proyecto de Ley, que pueden ser cuestionables, por las siguientes razones:

- Consentimiento; es un acto jurídico
- Aplicación favorable al titular; si es un principio, pero es más aplicable en el derecho del trabajo.
- Independencia de control es una condición en la organización de la Autoridad.

No obstante que los tres últimos principios del Proyecto de Ley no tienen una rigurosidad aplicable a la protección de datos personales, no disminuyen las condiciones favorables del objeto de la misma, y podrían mantenerse.

Artículo del Proyecto de Ley sin análogo en el RGPD

Artículo 9. Juridicidad, lealtad y transparencia: Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su reglamento y la demás normativa y jurisprudencia aplicable. En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

Es este aspecto, es pertinente destacar los principales instrumentos internacionales en materia de protección de datos personales anteriores al RGPD [4], que han sido:

- La Declaración Universal de los Derechos Humanos (DUDH), adoptada en París el 10 de diciembre de 1948;
- La Declaración Americana de los Derechos y Deberes del Hombre, aprobada en Bogotá (Colombia) en 1948,
- El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos), adoptado en Roma el 4 de noviembre de 1950.
- Resolución 45/95 de la Asamblea General de las Naciones Unidas del 14 de diciembre de 1990, sobre principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales.
- Recomendaciones de 2013 del Organización para la Cooperación y Desarrollo Económico (OCDE)
- Consejo de Europa Convenio 108+ para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (2018).

4.2. Licitud del tratamiento

Artículo 6. Licitud del tratamiento
1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para **proteger intereses vitales del interesado** o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una **misión realizada en interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de **intereses legítimos perseguidos por el responsable del tratamiento** o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Artículo 10. Legitimidad
El tratamiento solo será legítimo y licito si se cumple con alguna de las siguientes condiciones:
l. Exista obligación en el ordenamiento Jurídico aplicable al responsable del tratamiento:
2. Por orden Judicial, resolución o mandato motivado de autoridad pública competente:
3. Para el ejercicio de las competencias y facultades establecidas en la Constitución, la Ley, instrumentos internacionales ratificados por el Ecuador y demás normativa aplicable a favor de las entidades pertenecientes al sector público, sus delegados y organizaciones de Derecho Internacional Público:
4. Para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado,
5. Para la ejecución de medidas precontractuales a petición del titular, excepto cuando prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares:
6. Por consentimiento del titular para el tratamiento de sus datos personales para una o varias finalidades específicas: o,
7. Para proteger intereses vitales, del interesado o de otra persona natural, como por ejemplo su vida, salud o integridad.

El Proyecto del Ley, presenta siete (7) condiciones de cumplimiento de la legitimidad, seis (6) de las cuales tienen plena coincidencia con los expuestos en el RGPD, tal como se señala a continuación:

1. obligación aplicable al responsable; con la condición c) cumplimiento de una obligación legal
2. orden judicial, resolución o mandato motivado de autoridad pública; sin concordancia
3. competencias y facultades de entidades públicas; con la condición e) misión realizada en interés público
4. obligaciones contractuales del responsable; con la condición f) intereses legítimos del responsable
5. medidas precontractuales a petición del titular; con la condición b) contrato en el que el interesado es parte
6. consentimiento del titular; con la condición a) consentimiento del interesado
7. proteger intereses vitales; con la condición d) proteger intereses vitales del interesado

La condición 4 del Proyecto de Ley puede ser perfeccionada con la puntualización como lo hace la condición f) del RGPD, esto es que se debe considerar ante todo los derechos fundamentales del titular.

Propuesta Nro. 12: Modificar apartado 4 del Articulo 10. Legitimidad
(…)
4. Para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado, *siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado*.

Los apartados 2, 3 y 4 del artículo 6 del RGPD no tienen artículos semejantes en el Proyecto de Ley porque detalla las condiciones para el Derecho de la Unión o el Derecho de los Estados miembros.

Artículo 11. Finalidad
Las finalidades del tratamiento deberán ser determinadas, explícitas y legítimas, no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad.

A pesar que el artículo 11 del Proyecto de Ley es concordante con el apartado 5.b del RGPD, el primero tiene una indeterminación *"a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad"*. La claridad del RGPD al respecto se encuentra en el apartado 89.1, respecto al tratamiento ulterior de datos con los fines siguientes:

a) archivo en interés público;
b) investigación científica e histórica;
c) estadísticos;

Propuesta Nro. 13: Modificar Articulo 11. Finalidad

Las finalidades del tratamiento deberán ser determinadas, explícitas y legítimas, no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, *a menos que el tratamiento ulterior de los datos personales tengan fines de: archivo en interés público; fines de investigación científica e histórica; o, fines estadísticos; pues estos no se considerarán incompatibles con los fines iniciales*.

Artículo 12. Pertinencia y Minimización de datos personales
Los datos personales deben ser pertinentes y limitados a lo mínimo necesario para su finalidad

El artículo 12 del Proyecto de Ley es concordante con el apartado 5.c del RGPD.

Artículo 13. Proporcionalidad del tratamiento:
El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recogidos o a la naturaleza de las categorías especiales de datos.

El artículo 13 del Proyecto de Ley también es concordante con el apartado 5.c del RGPD.

4.3. Condiciones para el consentimiento

Artículo 7. Condiciones para el consentimiento
1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el 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 de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 14. Consentimiento:
Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular de hacerlo.
El consentimiento será válido, cuando la manifestación de la voluntad sea: libre, es decir, que se encuentre exenta de vicios del consentimiento, especificidad, se refiere a la determinación concreta de los medios y fines del tratamiento, informada, aquella que cumple con el principio de transparencia y efectiviza el derecho a la transparencia; inequívoca, que no se presenten dudas sobre el alcance de la autorización otorgada por el titular; previa que el consentimiento se haya dado con anterioridad al tratamiento, ya sea en el momento mismo de la recogida del dato cuando se obtiene directamente del titular y excepcionalmente de forma posterior cuando los datos personales no se obtuvieren de forma directa; expresa, que de manera indubitable el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular.
El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento igual de sencillo que el que fue llevado para recabar el consentimiento.
El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

El consentimiento es una, pero no la única, base o justificación que legitima el tratamiento de datos personales [4]. No obstante existen situaciones en las que el consentimiento, además de inequívoco, deberá de ser explícito [3]:

- cuando se trata de categorías especiales de datos,
- en los supuestos de transferencias internacionales de datos,
- cuando el tratamiento de datos proyectado suponga la adopción de decisiones individuales automatizadas.

El Proyecto del Ley, presenta seis (6) características de la manifestación de la voluntad, para el cumplimiento del consentimiento: libre, específica (especificidad), informada, inequívoca, previa y expresa. Posteriormente el segundo párrafo sin numeración del artículo 14 tiene concordancia con el apartado 13.3 del RGPD respecto a la facultad de retirar el consentimiento en cualquier momento.
Sin embargo, el apartado 13.4 del RGPD que se refiere a los contratos para la prestación de servicios, no tiene un texto similar en el artículo 14, que podría considerarse sin consentimiento para la prestación de servicios.

Propuesta Nro. 14: Modificar Articulo 14. Consentimiento.

El consentimiento será válido, cuando la manifestación de la voluntad sea: libre, es decir, que se encuentre exenta de vicios del consentimiento, *lo que se incluye para la prestación de un servicio*; específico (…)
(…)
El consentimiento, además de inequívoco, deberá de ser explícito cuando se trata de: categorías especiales de datos; en los supuestos de transferencias internacionales de datos; y, cuando el tratamiento de datos proyectado suponga la adopción de decisiones individuales automatizadas.

Artículo 15. Confidencialidad.
El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no deben tratarse o comunicarse para un fin distinto para el cual fueron recogidos, sin que se cuente con el consentimiento del titular o concurra una de las causales que habiliten el tratamiento conforme al principio de legitimidad. El nivel de confidencialidad dependerá de la naturaleza del dato personal.
Este principio no implica solamente el mantenimiento de la seguridad de los datos personales, sino también la facultad del titular de controlar la forma en la que se tratan sus datos. Incluyendo la transferencia o comunicación

El artículo 15 del Proyecto de Ley también es concordante con el apartado 5.1.f del RGPD.

Artículo 16. Calidad
Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros; precisos; completos, comprobables; claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. La Autoridad de Protección de Datos Personales definirá los casos en los cuales se deberán actualizar los datos personales y su periodicidad.

El artículo 16 del Proyecto de Ley en parte es semejante al apartado 5.1.d del RGPD, difiere en que la Autoridad debe definir la actualización, esto estaría en contra del principio de proactividad del responsable, aspecto por el cual el responsable del tratamiento deberá actuar con la diligencia necesaria para hacer un buen uso de los datos [3]. Es pertinente eliminar el párrafo que otorga esa facultad exclusiva a la Autoridad de control.

Propuesta Nro. 15: Modificar Articulo 16. Calidad

Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros; precisos; completos, comprobables; claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad.

Artículo 17. Conservación.
Los datos personales serán conservados conforme a los siguientes presupuestos:
l. Durante el tiempo consentido, determinado en el ordenamiento jurídico o establecido en orden judicial, resolución o mandato motivado de autoridad pública competente; o,
2. Hasta cuando cumplan con la finalidad para la cual fueron recogidos o tratados.
Cumplido uno de los presupuestos establecidos, los datos personales deberán suprimirse o ser sometidos a un proceso de anonimización, de ser el caso. Para lo cual, el responsable implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura los datos personales.
El posterior tratamiento de datos personales únicamente se realizará para la investigación científica, histórica o estadística que se realice en favor del interés público, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales oportunas, así como las demás que contemple la presente Ley, su Reglamento de Aplicación o las Resoluciones de la Autoridad de Protección de Datos Personales, para salvaguardar los derechos contemplados en esta norma.

El artículo 17 del Proyecto de Ley en parte es concordante con el apartado 5.1.e del RGPD.

Artículo 18. Seguridad de datos personales:
Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, sean éstas técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

El artículo 18 del Proyecto de Ley en parte es concordante con el apartado 5.1.f del RGPD.

Artículo 19. Responsabilidad proactiva y demostrada:
El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y corregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.
El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales
El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

El artículo 19 del Proyecto de Ley en parte es concordante con el apartado 5.2 del RGPD.

Artículo 20. Aplicación favorable al titular:
En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractual, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

El artículo 20 del Proyecto de Ley no tiene un artículo análogo en el RGPD.

Artículo 21. Independencia de control:
Para el efectivo ejercicio del derecho a la protección de datos personales, el Estado ejercerá un control independiente, imparcial y autónomo, así como su regulación y sanción.

Es importante que se incluya como principio la independencia en el control a la par de las recomendaciones de todos los instrumentos internacionales, para la posterior definición de la Autoridad de Control que en consecuencia debería ser independiente de cualquier poder del Estado.

Artículo 22. Normativa especializada:
Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios de juridicidad, lealtad y transparencia; legitimidad; finalidad; confidencialidad: conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, en los casos que corresponda, y, de aplicación favorable.

Este artículo permite una amplia gama de posibilidades de que cada sector emita principios no concordantes con los establecidos en la Ley de Protección de Datos. En la sección disposiciones derogatorias es pertinente que se reforme lo necesario para que la aplicación de la ley sea uniforme en todo el ámbito de aplicación territorial. PO ejemplo, cuando el derecho a la protección de datos no requiere consentimiento, porque no es un derecho absoluto o ilimitado, sino que está sujeto a los límites previstos en la ley, que protege también otros derechos e intereses legítimos tales como la libertad de expresión, la propiedad intelectual o la salud pública [4]. En este sentido, la LOPDGDD dispone que a los tratamientos a los que no sea directamente aplicable el RGPD (por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea), se regirán por lo dispuesto en su legislación específica si la hubiere y como ejemplo de casos que se encuentran señala, expresamente los tratamientos: en el régimen electoral; en el ámbito de instituciones penitenciarias; y, los derivados del Registro Civil, los Registros de la Propiedad y Mercantiles [5].

Propuesta Nro. 16: Modificar.- Articulo 22. Normativa especializada

Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos,

desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, *estarán sujetos a los principios establecidos en la presente ley, sin perjuicio de las disposiciones de tal normativa especializada que le sean aplicables.*

4.4. Condiciones aplicables al consentimiento del niño

Artículo 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.
2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 36. Ejercicio de derechos: El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la Sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionada al uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.
Los adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal Los adolescentes mayores a dieciséis (16) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales y del tratamiento.
Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario.

El artículo 36 del Proyecto de Ley contempla lo establecido en el artículo 8 del RGPD, esto es, que para la oferta directa de servicios de la sociedad de la información a los niños, únicamente será válido el consentimiento del menor que tenga como mínimo 16 años. A pesar de que el RGPD establece el umbral de edad a partir del cual el menor puede consentir sin necesidad del titular de la patria potestad o tutela, deja abierta la posibilidad para que los países establezcan una edad inferior siempre que no sea inferior a 13 años. En el Proyecto de Ley indica que los niños con edad entre 12 y 16 años necesitan al representante, pero no la necesitan los adolescentes con edad entre 16 y 18 años. Existe concordancia en la edad mínima, 16 años.

4.5. Tratamiento de categorías especiales de datos personales

Artículo 9. Tratamiento de categorías especiales de datos personales
1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de

los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 38. Categorías especiales de datos personales: Se aplicará lo dispuesto en el presente capítulo al tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios, datos de salud y datos necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

Artículo 39. Consentimiento relativo a categorías especiales de datos: Además de los requisitos del consentimiento previstos en el artículo 13, se requiere de la manifestación de la voluntad explícita del titular para el tratamiento de datos sensibles, datos crediticios y de datos personales de adolescentes mayores a dieciséis (16) años y menores de dieciocho (18) años.
Para el caso de adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como de niñas y niños, es necesario contar con el consentimiento explícito y verificable de su representante legal. La Autoridad de Protección de Datos Personales definirá los parámetros de verificación del consentimiento Se entiende por consentimiento explícito 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.
El responsable o encargado del tratamiento de datos personales está en obligación de verificar si el titular o representante legal ha otorgado su consentimiento explícito para el tratamiento de datos sensibles, datos crediticios y en especial, datos de niñas, niños y adolescentes.

En el capítulo de definiciones el Proyecto de Ley define a los datos sensibles como: "*(…) 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.*"

Esta definición se asemeja a la de categoría especial de datos personales del RGPD, pero la estrategia de protección es distinta. El RGPD prohíbe el tratamiento de

categorías especiales de datos personales de todas las personas físicas, y establece excepciones [3] para dicha prohibición:

- el interesado ha dado el consentimiento explícito;
- cuando el tratamiento sea necesario para el cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad social,
- cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física
- cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales;
- cuando el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
- cuando el tratamiento sea necesario por razones de interés público;
- de manera excepcional cuando el tratamiento sea necesario para el ejercicio de acciones judiciales
- con fines de archivo en interés público, de investigación científica e histórica o estadística.

Por el contrario el Proyecto de Ley no prohíbe expresamente el tratamiento, sino que lo permite cuando existe un consentimiento del titular.
En este sentido, aunque el RGPD contempla la posibilidad de que los Estados Miembros de la UE puedan introducir condiciones adicionales, incluso limitaciones respecto al tratamiento de los datos genéticos, biométricos o los datos relativos a la salud; el mismo RGPD no recomienda eliminar prohibiciones expresas como lo hace el Proyecto de Ley.
A fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico [5].

Propuesta Nro. 17: Modificar.- Articulo 39. Consentimiento relativo a categorías especiales de datos
Queda prohibido el tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios, datos de salud.
Esta prohibición no será de aplicación cuando:
- el interesado ha dado el consentimiento explícito;
- el tratamiento sea necesario para el cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad social,
- el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física
- el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales;
- el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
- el tratamiento sea necesario por razones de interés público;
- de manera excepcional cuando el tratamiento sea necesario para el ejercicio de acciones judiciales
- con fines de archivo en interés público, de investigación científica e histórica o estadística.
(…)

4.6. Tratamiento de datos sobre condenas e infracciones penales

Artículo 10. Tratamiento de datos personales relativos a condenas e infracciones penales
El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

No existe un artículo similar en el Proyecto de Ley. Al respecto, existe una distinción entre: el tratamiento de datos de naturaleza penal, y el tratamiento del resto de datos de carácter personal (regulado por el RGPD). Por esto es importante, que de manera taxativa, se disponga que únicamente pueda llevarse un registro completo de condenas penales bajo el control de las autoridades públicas [5].

Propuesta Nro. 18: Añadir al final.- Articulo 39. Consentimiento relativo a categorías especiales de datos
(…)
El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

4.7. Tratamiento que no requiere identificación

Artículo 11. Tratamiento que no requiere identificación
1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.
2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

No existe un artículo similar en el Proyecto de Ley.

5. Derechos

5.1. Transparencia e información

Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Artículo 23. Derecho a la lealtad, transparencia e información.
17. (…)
Con el objeto de que pueda autorizar el tratamiento, transferencia o comunicación de sus datos personales, esta información deberá ser proporcionada al titular de forma accesible por cualquier medio, incluidas políticas de protección de datos personales, gratuitos; suficientes; disponibles de forma permanente y redactarse en un lenguaje claro, sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica.
En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas niños y adolescentes, la información a la que hace referencia el presente artículo será proporcionada a su representante legal conforme a lo dispuesto en el inciso precedente.

Concordancia con los dos párrafos sin numeración que se encuentran luego del apartado 23.17 del Proyecto de Ley

Desde el apartado 12.2 hasta el apartado 12.8 del RGPD, el Proyecto de Ley no dispone de concordancias en los aspectos relacionados con la actuación del responsable: cuando no se puede negar a actuar; plazos de prórrogas; cuando cobrar un canon; cuando puede negarse actuar; y, cuando debe confirmar la identidad del interesado.

5.2. Información de datos que se obtengan del interesado

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional (...)
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación

de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; 23.13
d) el derecho a presentar una reclamación ante una autoridad de control; 23.16
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos 23.11
3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 23. Derecho a la lealtad, transparencia e información. El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre.
l. Los fines del tratamiento;
2. Base legal para el tratamiento;
3. Tipos de tratamiento;
4. Tiempo de conservación;
5. La existencia de una base de datos en donde consten sus datos personales;
6. El origen de los datos personales cuando no se hayan obtenido directamente del titular;
7. Otras finalidades y tratamientos ulteriores;
8. Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluye: dirección de domicilio legal, número de teléfono y correo electrónico,
9. Identidad y datos de contacto del delegado de protección de datos personales, que Incluye: dirección domiciliaria a, teléfono y correo electrónico;
10. Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas;
11. Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;
12. El efecto de suministrar datos personales erróneos o inexactos;
13. La posibilidad de revocar el consentimiento:
14. La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas;
15. Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite:
16. Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales, y la
Autoridad de Protección de Datos Personales, y.
17. La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

El Proyecto del Ley, en su artículo 23 presenta diecisiete (17) aspectos sobre los cuales el titular tiene derecho a ser informado, de los cuales los siguientes tienen coincidencia con los expuestos en el artículo 13 del RGPD, tal como se señala a continuación:

El apartado 23.8; con el apartado 13.1a) datos del responsable.
El apartado 23.9; con el apartado 13.1b) datos del encargado.
Los apartados 23.1 y 23.2; con el apartado 13.1c) fines del tratamiento y base jurídica.
El apartado 23.10; con el apartado 13.1f) intención de transferencias internacionales.
El apartado 23.4; con el apartado 13.2a) plazo de conservación.
Los apartados 23.14 y 23.15; con el apartado 13.2b) rectificación o supresión.
El apartado 23.13; con el apartado 13.2c) retirar el consentimiento.
El apartado 23.16; con el apartado 13.2d) reclamación ante una autoridad.
El apartado 23.11; con el apartado 13.2e) consecuencias de que no facilitar datos.
El apartado 23.7; con el apartado 13.3 tratamiento ulterior.

5.3. Información de datos que no se obtengan del interesado

Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.
1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.
5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

De los diecisiete (17) aspectos del artículo 23 del proyecto de ley, los siguientes tienen coincidencia con los expuestos en el artículo 14 del RGPD:

El apartado 23.8; con el apartado 14.1a) datos del responsable.
El apartado 23.9; con el apartado 14.1b) datos del delegado.
Los apartados 23.1 y 23.2; con el apartado 14.1c) fines del tratamiento y base jurídica.
El apartado 23.10; con el apartado 14.1f) intención de transferencias internacionales.
El apartado 23.4; con el apartado 14.2a) plazo de conservación.
Los apartados 23.14 y 23.15; con el apartado 14.2c) rectificación o supresión.
El apartado 23.13; con el apartado 14.2d) retirar el consentimiento.
El apartado 23.16; con el apartado 14.2e) reclamación ante una autoridad.
El apartado 23.6; con el apartado 14.2f) origen de los datos.
El apartado 23.17; con el apartado 14.2g) existencia de decisiones automatizadas.
Párrafo sin numeración luego del 23.17; con el apartado 14.3a) plazo de un mes.

Constan en el proyecto pero no en el RGPD:
El apartado 23.3, tipos de tratamiento, sin concordancia.
El apartado 23.5, existencia de base de datos, sin concordancia.
El apartado 23.12, el efecto de suministrar datos personales erróneos o inexactos;

El apartado 23.3 podría ser reemplazado por la información acerca a los destinatarios o las categorías de destinatarios de los datos personales.
El apartado 23.5 podría ser reemplazado por la información acerca de los intereses legítimos de los responsables.

Propuesta Nro. 19: Reemplazar.- Articulo 23. Derecho a la lealtad, transparencia e información.
El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre:

Donde dice
3. Tipos de tratamiento
Reemplazar por
3. *La información de los intereses legítimos del responsable o de un tercero*

Donde dice:
5. La existencia de una base de datos en donde consten sus datos personales;
Reemplazar por:
5. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.

5.4. Derecho de acceso

Artículo 15. Derecho de acceso del interesado
1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:
a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.
3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
4. El derecho a obtener copia mencionada en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Artículo 24. Derecho de Acceso
El titular tiene derecho a conocer y a obtener del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna.
El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho.
En caso de que fuera necesario restringir o negar dicho acceso, deberán especificarse las razones concretas de dicha restricción o negativa de acuerdo a lo establecido en la normativa vigente.

El artículo 24 del Proyecto de Ley hace referencia al artículo 23 (original), por tanto tampoco contempla todas las posibilidades de acceso a la información que tendría el interesado, como las siguientes:
d) cuando el tratamiento se base en los intereses legítimos del responsable o de un tercero; y
e) los destinatarios o las categorías de destinatarios de los datos personales

Por otra parte la frase: *"El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho",* contiene un término subjetivo, "razonables", porque permite la aplicación de un criterio personal para el responsable del tratamiento: ¿qué es razonable? Además en el último párrafo del artículo 24, también permite al responsable negarse con el simple hecho de especificar sus razones concretas, pero sin especificar cuáles son los límites para esas motivaciones.

Para lo analizado anteriormente es factible tomar como referencia la Ley Orgánica 3/2018 LOPDGDD, que además de destinarse para adaptar al ordenamiento español al RGPD y completar sus disposiciones; si establece los métodos para el ejercicio del derecho al acceso del interesado, tal como se señala en su artículo 12 [3]:

- Su ejercicio es gratuito;
- Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá: cobrar un canon proporcional a los costes administrativos soportados; o negarse a actuar. El artículo 13 de la LOPDGDD considera repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello;
- Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más;

- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que se opte por otro medio;
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo;
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control;
- Se pueden ejercer los derechos directamente o por medio de un representante legal o voluntario;
- Cabe la posibilidad de que el encargado sea quien atienda la solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule;

Con esta referencia es sugerido que se agreguen al artículo del Proyecto de Ley, ciertas características importantes para el ejercicio del derecho de acceso.

Propuesta Nro. 20: Modificar Articulo 24. Derecho de Acceso.

El titular tiene derecho a conocer y a obtener del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna.
El responsable del tratamiento de datos personales deberá seguir las siguientes características para el ejercicio del derecho de acceso: tiene carácter gratuito; las respuestas a las solicitudes se deben entregar con un plazo máximo de 2 meses; se debe proporcionar e informar al titular sobre el medio acceso para recibir respuesta a la solicitud, la información se facilitará por medios electrónicos cuando sea posible.

El derecho de acceso a los datos personales en ningún caso afectará negativamente los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual, en particular la propiedad intelectual que protege los sistemas informáticos. No obstante, en ningún caso puede negarse a ofrecer información al titular.
Únicamente si las solicitudes son manifiestamente infundadas o excesivamente repetitivas (en más de una ocasión durante del plazo de seis meses), el responsable podrá: cobrar un canon proporcional a los costes administrativos soportados; o, negarse a actuar, para lo cual deberá presentar los fundamentos legales para dicha negativa, lo que informará al titular a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.

5.5. Derecho de rectificación

Artículo 16. Derecho de rectificación
El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 25. Derecho de Rectificación y Actualización: El titular tiene el derecho de solicitar se corrijan o actualicen sus datos inexactos, incompletos, desactualizados, erróneos, falsos, incorrectos o imprecisos.

El artículo 25 del Proyecto de Ley es concordante con el artículo 16 del RGPD.

5.6. Derecho de supresión u olvido

Artículo 17. Derecho de supresión («el derecho al olvido»)
1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
d) los datos personales hayan sido tratados ilícitamente;
e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 26. Derecho de Eliminación: El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de que estos dejen de ser tratados por el responsable del tratamiento de datos personales, cuando:
1. El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;
2. El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
3. Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4. Haya vencido el plazo de conservación de los datos personales;
5. El tratamiento afecte derechos fundamentales o libertades individuales; o
6. Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.
El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Artículo 27. Derecho al olvido digital. El titular tiene el derecho a solicitar al juez competente, obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales que estén siendo tratados en el entorno digital, cuando concurra alguna de las circunstancias siguientes:
1. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados;
2. El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión.
3. El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;
4. Los datos personales hayan sido tratados ¡lícitamente.
5. Los datos personales sean de carácter obsoleto;
6. Lo; datos personales no tengan valor histórico o científico;
7. Los datos personales no sean de relevancia pública; o.
8. Los datos personales sean inadecuados, inexactos, impertinentes o excesivos con relación a los fines y al tiempo transcurrido
Lo anterior no se aplicará cuando el tratamiento sea necesario por cualquiera de las siguientes causas.
1. Para ejercer el derecho a la libertad de expresión e información;
2. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos por parte del responsable del tratamiento,
3. Por razones de Interés público en el ámbito de la salud pública;
4. Con fines de archivo en interés público, fines de investigación Científica o histórica o fines estadísticos; o,
5. Para la formulación, el ejercicio o la defensa de reclamaciones

Para la aplicación del presente artículo, se estará a las siguientes definiciones:
Datos personales tratados en el entorno digital: Datos personales que son tratados en redes de computadoras públicas o privadas (Internet o Intranet). Se entiende por redes privadas aquellas que no están abiertas al acceso de todo público pero que si son usadas por una colectividad de usuarios autorizados.

Datos personales de carácter obsoleto: Datos personales que ya no están en uso, son antiguos, anticuados o han dejado de tener vigencia o relevancia para los fines del tratamiento.
Datos personales que no tengan valor histórico o científico: Datos personales que no son útiles, necesarios o de valor significativo para la ciencia o la historia política o social de Ecuador.
Datos personales que no sean de relevancia pública**:** Datos personales que el público en general no necesita o no tiene interés justificado en conocer.

El derecho al olvido permitiría objetar publicaciones que afecten a personas contra motores de búsqueda, los usuarios podrían solicitar que su información personal o que afecte a su persona sea eliminado inmediatamente o se utilice herramientas técnicas que neutralicen la posibilidad de libre acceso [22].

El tema del "olvido digital" se podría dificultar con las tecnologías emergentes como el "blockchain" que se caracteriza por la inmutabilidad e inalterabilidad de la información registrada y tiene el objeto de evitar cualquier modificación una vez que, un dato ha sido publicado para evitar la reutilización. En este contexto, si la información registrada incorpora datos de carácter personal y el titular de los mismos ejercitase su derecho al olvido, los especialistas señalan que, esta rectificación o supresión o borrado de datos no solo sería técnicamente muy difícil y costoso, sino que además afectaría a la propia seguridad del sistema [23]. Este aspecto cabría en un posterior análisis para que la ley excluya a las cadenas de bloques de la tecnología "blockchain" de la aplicación de dicho derecho.

El Proyecto de Ley, propone dos artículos (26 y 27) y cuatro definiciones a continuación de los dos artículos. Como primera observación en el aspecto de presentación y claridad de texto, es más adecuado presentar todas las definiciones en la sección correspondiente. En el mismo sentido, el articulo 27 tiene dos párrafos uno para cuando aplicaría la supresión y otro para cuando no aplicaría la supresión, esto puede representar una dificultad para la citación de texto jurídicos, y por tanto es más adecuado agregar numeración por caso de aplicación y literales para los causas de cada aplicación.

En el análisis de concordancia entre las causas que constan en el Proyecto de Ley (en los artículos 27 y 27) y en el RGPD (artículo 17), se encuentra:

Para la aplicación de la supresión:
Los apartados 26.2, y 27.1 del primer párrafo; concordantes con el apartado 17.1a) necesidad con relación a los fines.
Los apartados 26.6, y 27.2 del primer párrafo; concordantes con el apartado 17.1b) retiro del consentimiento.
El apartado 27.3 del primer párrafo; concordante con el apartado 17.1c) oposición al tratamiento.
El apartado 27.4 del primer párrafo; concordante con el apartado 17.1d) tratamiento ilícito.
No existe causa similar a la establecida en el apartado 17.1.f) oferta de servicios de la sociedad de la información para menores de edad

Para la no aplicación de la supresión:
El apartado 27.1 del segundo párrafo; concordante con el apartado 17.3a) derecho a la libertad de expresión.

El apartado 27.2 del segundo párrafo; concordante con el apartado 17.3b) cumplimiento de una obligación legal.
El apartado 27.3 del segundo párrafo; concordante con el apartado 17.3c) interés público.
El apartado 27.4 del segundo párrafo; concordante con el apartado 17.3d) archivo, investigación y estadística.
El apartado 27.5 del segundo párrafo; concordante con el apartado 17.3e) reclamaciones.

Los dos artículos (26 y 27) se solapan en su redacción con respecto al tema que "el titular tiene derecho a la supresión de sus datos personales", la única diferencia radica en que en el derecho de eliminación la solicitud de dicha supresión se realiza al responsable, mientras que en el derecho al olvido digital la solicitud se realiza a un juez competente, pero la finalidad es la misma porque la eliminación de datos personales tienen como consecuencia el olvido digital. Además en la redacción del artículo del proyecto no se cita a los datos personales que se han obtenido en relación con la oferta de servicios dirigidos a menores.

Propuesta Nro. 21: Unificar los Artículos 26 y 27, renombrar, cambiar numeración y ampliar.
Derecho de supresión o derecho al olvido.

El titular tiene el derecho a solicitar al responsable del tratamiento o al juez competente, la supresión de sus datos personales que estén siendo tratados, a fin de que éstos, sin dilación indebida, dejen ser tratados.

1. Se puede realizar dicha solicitud cuando concurra alguna de las circunstancias siguientes:
a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados;
b) El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión;
c) El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;
d) Los datos personales hayan sido tratados ilícitamente;
e) Los datos personales sean de carácter obsoleto;
f) Lo; datos personales no tengan valor histórico o científico;
g) Los datos personales no sean de relevancia pública;
h) Los datos personales sean inadecuados, inexactos, impertinentes o excesivos con relación a los fines y al tiempo transcurrido; o
i) los datos personales se han obtenido en relación con la oferta de servicios dirigidos a menores.
El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

2. Lo anterior no se aplicará cuando el tratamiento sea necesario por cualquiera de las siguientes causas:
a) Para ejercer el derecho a la libertad de expresión e información;
b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos por parte del responsable del tratamiento;
c) Por razones de interés público en el ámbito de la salud pública;

d) Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; o,
e) Para la formulación, el ejercicio o la defensa de reclamaciones.

5.7. Derecho a la limitación del tratamiento

Artículo 18. Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.
2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.
3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 32. Derecho a la limitación del tratamiento.
El titular tendrá derecho a que se use el mínimo de sus datos personales en el tratamiento efectuado por responsables o encargados del tratamiento de datos personales, a que sus datos personales no se encuentren disponibles en internet u otros medios de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los titulares o a los autorizados por razones de interés público; a que el tratamiento de datos personales se limite al periodo que medie entre una solicitud de revisión de juridicidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento o, de no ser objeto de una decisión basada únicamente en valoraciones automatizadas, hasta su resolución por el responsable o encargado del tratamiento de datos personales.
De existir negativa por parte del responsable o encargado del tratamiento de datos personales, y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta limitación se extenderá hasta la resolución del procedimiento administrativo.
El responsable del tratamiento de datos personales conservará únicamente los datos personales que sean necesarios para la formulación de un reclamo, una vez cumplido el plazo o condición del tratamiento.

La limitación del tratamiento señalada en el RGPD se refiere a suspender el tratamiento de los datos en el futuro, esto provocaría por ejemplo: trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a los datos personales seleccionados, o retirar temporalmente los datos publicados de un sitio web. La limitación deber realizarse por medios técnicos, imposibilitando cualquier operación de tratamiento [3]. En definitiva la limitación se refiere al factor tiempo.

Por otra parte en el Proyecto de Ley, la limitación hace relación al uso mínimo o a un caso específico de ubicación cuando se señala: *"(…) a que sus datos personales no se encuentren disponibles en internet (…)".* En tal virtud, el texto no correspondería al derecho a limitación de tratamiento, sino que correspondería al derecho supresión u olvido.

En el RGPD se establece condiciones para que el titular pueda ejercer este derecho, sin embargo en el Proyecto de Ley simplemente se añade dos excepciones: que sea técnicamente controlable, y que se realice en el periodo de la revisión de otro derecho.

El derecho de limitación no puede ser ilimitado en tiempo, porque se convertiría en el derecho a oposición, por esto es necesario que se precisen las condiciones requeridas para su aplicación, y se separe: cuándo es posible solicitar la suspensión del tratamiento de los datos, y cuándo es posible solicitar al responsable la conservación los datos [3]. La limitación por causa de falta de exactitud, tiene gran relevancia, por ejemplo como lo señala el caso de la Resolución 2789/2015 de la Agencia Española de Protección de Datos en la que el hecho imputado consistió en asociar los datos personales de la denunciante a una deuda de la que no era titular, y tal asociación de datos de carácter personal era claramente inexacta [5].

Propuesta Nro. 22: Modificar Artículo 32. Derecho a la limitación del tratamiento.

1. El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
a) Se impugne la exactitud de los datos personales,
b) El interesado se haya opuesto al tratamiento de los datos personales que el responsable realiza en base al interés legítimo o misión de interés público.

2.- El titular tendrá derecho a obtener del responsable del tratamiento la conservación los datos, cuando:

a) El tratamiento sea ilícito y el interesado se ha opuesto a la supresión de sus datos;
b) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento
El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

No existe artículo o texto similar en el Proyecto de Ley. Es factible que se establezca la obligación de notificación en algún documento de menor jerarquía elaborado por la Autoridad de Protección de Datos.

5.8. Derecho a la portabilidad

Artículo 20. Derecho a la portabilidad de los datos
1.El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.
2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Artículo 30. Derecho a la portabilidad: El titular tiene derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; y/o transmitirlos a otros responsables.
El titular podrá solicitar la transferencia o comunicación de sus datos personales a otro responsable del tratamiento. Luego de completada la transferencia, el responsable que transfiere dichos datos procederá a su eliminación.
Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:
l. Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, la transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible;
2. Que el tratamiento se efectúe por medios automatizados;
3. Que se trate de un volumen relevante de datos personales: o,
4. Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas.
No procederá este Derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el

titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

El Proyecto de Ley indica que "*se produzca al menos una de las siguientes condiciones*", esto quiere decir que no será necesario la ocurrencia simultánea de todas las condiciones para que se pueda portar los datos, por ejemplo: sin que haya existido el consentimiento previo con tal que exista un volumen relevante de datos, se puede transmitir los datos a otro responsable. Por su parte, en el RGPD se puede aplicar el derecho de portabilidad con el cumplimiento simultáneo de las dos condiciones: existencia del consentimiento previo "y" que se trate por medios automatizados.

Por tanto, en el Proyecto de Ley, se generarían obligaciones que pueden superar la capacidad de los responsables del tratamiento, por ejemplo cuando los datos no se encuentren en medios automatizados y el titular solicite la transmisión de los mismos aunque esto no sea técnicamente factible.

El Proyecto de Ley agrega dos características: esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas. También agrega una excepción: cuando se trate de información obtenida a partir del tratamiento sometido a un proceso de creación de perfiles; sin embargo, el artículo del proyecto carece de todas las excepciones del apartado 20.3 del RGPD, como son: misión en interés público o en el ejercicio de poderes públicos.

Propuesta Nro. 23: Modificar Artículo 30. Derecho a la portabilidad.
(…)
1. Para que proceda el derecho a la portabilidad de datos es necesario que se produzcan las *siguientes condiciones*:
a) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, la transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; *y*
b) Que el tratamiento se efectúe por medios automatizados.
Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas.

2. No procederá este derecho cuando:
a) el tratamiento sea necesario para el cumplimiento de una *misión realizada en interés público* o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
b) afecte negativamente a los derechos y libertades de otro;
c) se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

5.9. Derecho de oposición

Artículo 21. Derecho de oposición
1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o

f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 28. Derecho de oposición: El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoraciones o decisiones automatizas, incluida la elaboración de perfiles.

El Proyecto de ley describe el derecho de oposición de forma muy escueta, lo que complicaría su aplicación porque limita la importancia del detalle. La palabra "*en especial*", le da un carácter general, casi ilimitado de oposición a cualquier tipo de tratamiento, por su parte el RGPD enmarca esta posibilidad de oposición en casos específicos: cuando el tratamiento es para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento; y, oposición en todo momento cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa. Es importante definir sin generalidades las excepciones.

Propuesta Nro. 24: Modificar Artículo 28. Derecho de oposición.
El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, cuando:
1. el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
2. el tratamiento es para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento; en cuyo caso el responsable dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

5.10. Decisiones individuales automatizadas

Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles
1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
c) se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas:
El titular tiene derecho a no ser sometido a una decisión basada únicamente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:
l. Solicitar una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;
2. Presentar observaciones;
3. Solicitar los criterios de valoración sobre el programa automatizado; y/o.
4. Impugnar la decisión ante el responsable o encargado de tratamiento
No se aplicará este derecho cuando:
1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales:
2. Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad pública competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o.
3. Se base en el consentimiento del titular.

En el Proyecto de Ley no se obliga al responsable a adoptar las medidas para salvaguardar los derechos, libertades y los intereses legítimos del interesado; y, principalmente omite que las condiciones para la no aplicación del derecho no pueden ser consideradas si se trata de las categorías especiales de datos personales, esto debe limitarse de forma explícita.

Propuesta Nro. 25: Añadir al final del Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas

(…)
Para esto, el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
Estas decisiones no se pueden aplicar si se trata de las categorías especiales de datos personales.

5.11. Limitaciones

Artículo 23. Limitaciones
1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:
a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
f) la protección de la independencia judicial y de los procedimientos judiciales;
g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);
i) la protección del interesado o de los derechos y libertades de otros;
j) la ejecución de demandas civiles.
2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a: (…)

Artículo 31. Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad:
No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad, en los siguientes casos:
l. Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;
2. Para el cumplimiento de una obligación legal o contractual;
3. Para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente,
4. Para la formulación, ejercicio o defensa de reclamos o recursos,
5. Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros;

6. Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso debidamente notificadas;
7. Para ejercer el derecho a la libertad de expresión y opinión;
8. Para proteger el interés vital del interesado o de otra persona natural;
9. En los casos en que medie el interés público; o,
10. En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística

La mayoría de limitaciones a la aplicación de los derechos son coincidentes en los dos artículos analizados.

En el Proyecto de Ley, un caso de excepción para el ejercicio de los derechos señala: *"para ejercer el derecho a la libertad de expresión y opinión*". Al respecto, se debería diferenciar que:
- cuando se aplique los derechos de: actualización, rectificación y portabilidad, no provoca que se deje de tratar los datos personales; pero,
- con la aplicación de los derechos de: eliminación, oposición y anulación si se podría impedir el ejercicio del derecho de libertad de expresión.

Otro caso de excepción señalado es: "*cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros*". En este aspecto, el Proyecto omite en todo el texto del documento la definición de los "intereses legítimos". Este es un tema de importancia porque en la práctica siempre deberá realizarse una evaluación y ponderación entre el interés legítimo de un tercero y los derechos y libertades de los titulares; así el RGPD cita algunos ejemplos de interés legítimo del responsable [3]:

a) la prevención del fraude cuando el tratamiento de datos personales es estrictamente necesario;
b) el tratamiento con fines de mercadotecnia directa;
c) el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información;
d) el interés legítimo podría ser la transmisión de datos personales dentro de un grupo empresarial para fines administrativos internos.

Por lo expuesto, los intereses legítimos de terceros deberían estar definidos y debe precautelarse sus derechos fundamentales, caso contrario pondría en conflicto los derechos legítimos de terceros contra los derechos del titular de los datos personales. Previsión que no debería ser de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones [5].

Propuesta Nro. 26: Modificar Artículo 31. Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad:
(…)
5. Cuando se pueda causar perjuicios *a derechos fundamentales de terceros*;
6. Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso debidamente notificadas;
7. *En el caso específico de los derechos de eliminación, oposición y anulación, cuando se opongan al derecho a la libertad de expresión y opinión***;** (…)

El Proyecto de Ley presenta 2 derechos adicionales que no constan en el RGPD:

Artículo 34. Derecho de consulta: Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la presente ley

El Registro Nacional de Protección de Datos Personales se define posteriormente en el artículo 90, no es en sí mismo un derecho como los anteriores, sino más bien es una posibilidad de consulta.

Artículo 35. Derecho a la educación digital: Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados al uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales.
El órgano rector de la educación, en coordinación con la Autoridad de Protección de Datos, emitirá las directrices para que las entidades educativas garanticen el enfoque de derechos antes mencionados de manera transversal en el currículo nacional en todos los niveles educativos. Se deberán emprender proyectos orientados a la prevención de situaciones de riesgo derivadas de la inadecuada utilización de las tecnologías de la información y comunicación, con especial atención a las situaciones de violencia en la red.
El cuerpo docente deberá ser formado y capacitado en competencias digitales para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
Los planes de estudio de los títulos universitarios, en especial aquellos que habiliten el desempeño profesional relacionado con la formación de niñas, niños y adolescentes, garantizarán el conocimiento en el uso y seguridad de los medios digitales y en el efectivo ejercicio de los derechos fundamentales en Internet.

Se puede encontrar una referencia en el artículo. 83 de la LOPDGDD que contempla el mismo mandato para las instituciones educativas españolas:

1) Incluyan en el bloque de asignaturas de la competencia digital
2) Formar adecuadamente al profesorado
3) Esa inclusión afecta igualmente a la enseñanza universitaria.

Artículo 37. Excepción por normativa especializada: No proceden los derechos establecidos en esta ley, para los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente En estos casos, los titulares podrán ejercer los derechos previstos en dicha normativa especializada.

La Ley de Protección de Datos Personales debe conciliar las otras leyes que establecen distintos tratamientos para los datos personales y no desestimar con un solo artículo todos los derechos de protección de datos personales. El Proyecto de Ley contempla excepciones de aplicación por efectos del interés público y la seguridad del Estado. Como se comentó en el análisis del artículo 22, con el Proyecto de Ley se puede adecuar los artículos de normativa especializada para que sean concordantes con los nuevos derechos establecidos para la protección de datos personales.

Propuesta Nro. 27: Modificar.- Articulo 37. Excepción por normativa especializada

Para los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias, *estarán sujetos a los principios, limitaciones y excepciones establecidas en la presente ley.*

Artículo 42. Datos de personas fallecidas: Los titulares de derechos sucesorios del fallecido, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante.
Las personas o instituciones que el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso su rectificación, actualización o eliminación.
En caso de fallecimiento de niñas, niños, adolescentes o personas a las que la Ley reconoce como incapaces, las facultades de acceso, rectificación y actualización o eliminación, podrán ejercerse por quién hubiese sido su último representante legal.
El ejercicio de este derecho estará regulado en el Reglamento a la presente Ley.

El RGPD indica en el considerando número 27, que el mismo no se aplica a la protección de datos personales de personas fallecidas. Sin embargo el mismo Reglamento posibilita a los estados miembros de la Unión Europea establecer normas relativas al tratamiento de datos de personas fallecidas, en este sentido, la LOPDGDD en el artículo 3 permite que las personas vinculadas al fallecido por razones familiares (herederos digitales), además de dirigirse al responsable o encargado del tratamiento para comunicar su fallecimiento, puedan solicitar a éstos el acceso a los datos personales del difunto (cuentas, perfiles en redes sociales, a su vida o identidad digital) y, en su caso, a su rectificación o supresión [23]. Por esta razón también se ha propuesto anteriormente en este trabajo, la modificación del artículo 4 para considerar este particular que se contempla en el citado artículo 42 del Proyecto de ley.

Artículo 43. Tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística: Para el tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado catalogados como tal por la ley de la materia, la investigación científica; histórica; o, estadística se sujetará a lo previsto a la normativa aplicable, y subsidiariamente a lo dispuesto en la presente Ley, su Reglamento y demás normativa dictada por la Autoridad de Protección de Datos Personales.

Artículo 44. Datos crediticios: La protección de datos personales crediticios se sujetará a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

Artículo 45. Datos relativos a la salud. Las instituciones y centros sanitarios públicos y privados, así como los profesionales correspondientes, podrán tratar datos personales relativos a la salud de sus pacientes. De acuerdo a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

Los artículos anteriores son los finales del capítulo III del Proyecto de Ley, éstos definen nuevamente lo señalado en la categoría especial de datos personales y citan la aplicación de la ley del sector respectivo. Al respecto, para los datos personales en sistemas de información crediticia, el artículo 20.1 de la LOPDGDD permite el tratamiento de datos personales relativos al incumplimiento de obligaciones financieras o de crédito mediante sistemas de información crediticia, y establece que, salvo prueba en contrario, se presume lícito el tratamiento de los datos personales relacionados con este tipo de operaciones [5], en este sentido, no se considera necesaria ninguna modificación porque prevalece la presunción de licitud.

A continuación, el capítulo IV del Proyecto de Ley, se denomina "Transferencia o comunicación y acceso a datos personales por terceros", contiene cuatro artículos (del 46 al 49) que se refieren al encargado de tratamiento.

Artículo 46. Transferencia o comunicación de datos personales. Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario y, además, se cuente con el consentimiento del titular.

Artículo 47. Acceso a datos personales por parte de terceros. El acceso de un tercero a datos personales, no se considerará transferencia o comunicación, siempre que sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas condiciones, será considerado encargado de tratamiento.
El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en donde se establezca de manera clara y precisa que el encargado del tratamiento de datos personales únicamente tratará los mismos conforme las instrucciones del responsable y que no los aplicará o utilizará para finalidades diferentes a las que figuren en el contrato, ni que los transferirá o comunicará, ni siquiera para su conservación, a otras personas.
Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales.
El tercero será responsable de las infracciones derivadas de incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

El encargado debería tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, sin embargo el último párrafo del artículo 47 del Proyecto de Ley, después de efectuarse la transferencia de los datos, le entrega la responsabilidad al encargado ante posibles infracciones. Sin embargo, lo que habría incumplido es el contrato con el responsable, pero la responsabilidad sobre el tratamiento sigue siendo del responsable, a excepción que le encargado por su cuenta defina tratamientos distintos a los establecidos en la relación contractual.

Propuesta Nro. 28: Eliminar último párrafo.- Articulo 47. Acceso a datos personales por parte de terceros
(…)
Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales.

Artículo 48. Excepciones de consentimiento para la transferencia o comunicación de datos personales:

No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:
l. Cuando los datos han sido recogidos de fuentes accesibles al público;
2. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con bases de datos.
En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;
3. Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente;
4. Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados, y,
5. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud.
Cuando, sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, éste puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna.
La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de disociación.

Artículo 49. Falta de consentimiento para la transferencia o comunicación de datos personales. Se entenderá que no hubo consentimiento para la transferencia o comunicación de datos personales cuando el responsable del tratamiento no haya entregado información suficiente al titular, que le permita conocer la finalidad a que se destinarán sus datos o el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

6. Responsable, Encargado y Delegado de Tratamiento

6.1. Responsabilidad del responsable del tratamiento

Artículo 24. Responsabilidad del responsable del tratamiento
1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

En el Proyecto de Ley no se desarrolla algún artículo que establezca claramente la responsabilidad del responsable. En los artículos anteriormente citados (del 46 al 49) se establece las mismas obligaciones para las dos figuras: responsable y encargado.

El responsable decide sobre el tratamiento de los datos personales que ha recogido, así como la finalidad para la que se van a utilizar, los destinatarios con los que se van a compartir, su período de conservación, entre otras cuestiones del tratamiento de datos [3]. El encargado (empresas de marketing, gestorías contables, empresas de hosting, empresas de servicios informáticos, etc.), salvo que decidan por su cuenta las finalidades, no son responsables del tratamiento.

En el artículo 71 del proyecto de ley se detallan las obligaciones del responsable.

Artículo 71. Obligaciones del responsable del tratamiento de datos personales: El responsable del tratamiento está obligado a:
1. Tratar datos personales en estricto apego a los **principios** y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
2. Aplicar e implementar requisitos y **herramientas** administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar *y* demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia**;**
3. Aplicar e implementar procesos de **verificación**, evaluación y valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
4. Implementar **políticas** de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
5. Adherirse a **códigos** de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales.
6. Utilizar metodologías de **análisis *y* gestión de riesgos** adaptadas a las particularidades del tratamiento y de las partes involucradas;
7. Realizar **evaluaciones de adecuación al nivel** de seguridad previa al tratamiento de datos personales;
8. Tomar **medidas tecnológicas**, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.
9. **Notificar** a la Autoridad de Protección de Datos Personales y al titular de **violaciones** a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
10. Implementar la protección de datos personales desde el **diseño *y* por defecto**;
11. Suscribir contratos de **confidencialidad** *y* manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
12. Elegir y **designar el encargado** del tratamiento de datos personales que ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y

regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
13. **Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales**, de conformidad a lo dispuesto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;
14. **Designar al Delegado** de Protección de Datos Personales;
15. Permitir y contribuir a la realización de **auditorías o inspecciones**, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,
16. Los demás establecidos en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Existe concordancia en:
Los apartados 71.2 71.3 71.8 con el apartado 24.1: medidas técnicas y organizativas.
El apartado 71.4 con el apartado 24.2: políticas de seguridad.

No existe concordancia en:
El apartado 71.5, la obligación de adherirse a códigos de protección, se contradice con el artículo 61 donde se establece que esto es de carácter voluntario, se deberá eliminar el apartado 71.5
El apartado 71.13, la obligación de registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, se contradice con el artículo 90 del mismo Proyecto de Ley, en el cual se establece que el responsable únicamente reporta a la Autoridad de Control, lo que implica que dicha Autoridad tiene la obligación de mantener actualizado el Registro, y que la obligación del responsable es reportar los cambios para el registro correspondiente.

Si bien las otras obligaciones no están detalladas en las responsabilidades del RGPD, éstas no se contraponen a las que se desarrolla a lo largo del cuerpo normativo europeo ni del Proyecto de Ley.

Propuesta Nro. 29: Modificar Articulo 71.
Obligaciones del responsable del tratamiento de datos personales.

Eliminar:
5. Adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales.
13. Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales.

6.2. Protección de datos desde el diseño

Artículo 25. Protección de datos desde el diseño y por defecto
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y

organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 52. Protección de datos personales desde el diseño y por defecto: **El responsable y el encargado** implementarán las medidas técnicas, organizativas y de cualquier otra índole con miras a garantizar que los procesos y medios de tratamiento protejan los datos personales desde su diseño, así como sus configuraciones se encuentren por defecto en cumplimiento de las disposiciones de la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

En el RGPD se ratifica lo establecido en la sección de principios "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)",* es decir, se asigna tal responsabilidad al responsable. Sin embargo el artículo 52 del Proyecto sintetiza de una manera muy breve los artículos 24 y 25 del RGPD y nuevamente involucra al responsable "y" al encargado. Como se ha mencionado anteriormente, esto no se considera correcto porque el encargado trata los datos por cuenta del responsable, luego de que el responsable haya definido la finalidad del tratamiento y lo haya elegido como encargado.

Deben considerarse las dinámicas y el funcionamiento del mundo digital ya que en ocasiones establecer a una organización encargada del tratamiento como corresponsable puede ser cuestionable, sobre todo desde el punto de vista que esta doble asignación de responsabilidad, desmotiva la innovación tecnológica y la oferta de servicios digitales que realizan los encargados [4].

Propuesta Nro. 30: Modificar Articulo 52. Protección de datos personales desde el diseño y por defecto
El responsable implementará las medidas técnicas, organizativas y de cualquier otra índole con miras a garantizar que los procesos y medios de tratamiento protejan los datos personales desde su diseño (…)

6.3. Corresponsables del tratamiento

Artículo 26. Corresponsables del tratamiento
1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los

corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.
2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.
3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Los corresponsables del tratamiento deben tener una participación concreta e demostrada en la determinación de los fines y medios del tratamiento de los datos personales. Esta figura no está identificada en el Proyecto de Ley.

El responsable del tratamiento, en algunos casos con la ayuda del encargado, establecerá la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado con referencia a la naturaleza, ámbito, contexto y finalidades que entraña el tratamiento que pretende realizar para los derechos y libertades para las personas físicas [3]. El encargado puede brindar ayuda, pero por defecto no es corresponsable. El encargado se convierte en responsable únicamente al haber definido por su cuenta las finalidades del tratamiento.

Sobre este asunto se pronunció el Abogado General Bobek señalando para el caso de un administrador de una página web que ha insertado en su página web un componente de software (plug-in) de un tercero (botón «Me gusta» de Facebook) que genera la recogida y transmisión de datos personales del usuario, que debe ser considerado corresponsable del tratamiento, conjuntamente con dicho tercero. No obstante, esa responsabilidad conjunta debe limitarse a aquellas operaciones respecto de las cuales decide efectivamente de manera conjunta sobre los medios y los fines del tratamiento de los datos personales [5].

El responsable debe realizar un control a la relación de encargo de tratamiento que implica la presencia de un contrato de encargo que defina las condiciones del tratamiento, finalidades, obligaciones, etc. [3]. El encargado, puede ayudar al responsable a garantizar el cumplimiento de las obligaciones previstas en el RGPD, esto es, respecto de la seguridad de los datos y la evaluación de impacto sobre la protección de datos [3].

Artículo 27. Representantes de responsables o encargados del tratamiento no establecidos en la Unión

Cuando el tratamiento se realiza por parte de un responsable o encargado no establecido en la Unión sobre datos personales de interesados que residan en la Unión, en actividades relativas a la oferta de bienes o servicios, se requiere que el responsable o el encargado del tratamiento designe un representante en la Unión. Según el ámbito de aplicación territorial del Proyecto de Ley, el artículo no sería aplicable, sin embargo para el caso de transferencias internacionales es posible incluir la figura de los representantes establecidos en el Ecuador.

6.4. Encargado del tratamiento

Artículo 28. Encargado del tratamiento
1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.
2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
c) tomará todas las medidas necesarias de conformidad con el artículo 32 (seguridad del tratamiento);
d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente

Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.
4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3. en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.
5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.
6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.
7.La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.
9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.
10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 72. Obligaciones del encargado del tratamiento de datos personales: El encargado del tratamiento de datos personales está obligado a:
1. Tratar datos personales en estricto apego a los principios *y* derechos desarrollados en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Tratar datos personales de conformidad a lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional, salvo que esté obligado a hacerlo en función al principio de legitimidad; de ser este el caso, deberá informar al responsable del tratamiento de datos personales;
3. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o con quién tenga conocimiento de los datos personales;

4. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5. Implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar vulneraciones;
6. Asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;
7. Asistir al responsable para garantizar el cumplimiento de las obligaciones previstas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
8. Transferir o comunicar los datos personales entregados al responsable del tratamiento y suprimirlos, una vez que haya culminado su encargo;
9. Facilitar el acceso al responsable del tratamiento de datos personales de toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley, en su reglamento, en directrices, lineamientos *y* regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.
10. Permitir y contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de un auditor autorizado por éste o por la Autoridad de Protección de Datos Personales;
11. Cumplir el código de protección, mecanismos de certificación o sellos aprobados para demostrar la existencia de garantías suficientes para la protección de datos personales; y,
12. Las demás establecidas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Concordancias:
El apartado 72.2 con el párrafo sin número del apartado 28.3: contrato o acto jurídico.
El apartado 72.3 con el apartado 28.3b) confidencialidad.
Los apartados 72.3, 72.4, 72.5 y 72.11 con el apartado 28.3c) seguridad del tratamiento.
El apartado 72.6 con el apartado 28.3e) asistencia al responsable.
El apartado 72.7 con el apartado 28.3f) ayuda en cumplimiento de obligaciones.
El apartado 72.8 con el apartado 28.3g) suprimir o devolver los datos.
Los apartados 72.9 y 72.10 con el apartado 28.3h) disponibilidad de la información para el responsable.

En el RGPD se detallan varias funciones del encargado, como el apartado 10, que ratifican el criterio anterior, esto es, que el encargado, por defecto, no puede compartir la responsabilidad, y tampoco puede ni debe determinar las finalidades del tratamiento y en consecuencia no puede ser responsable.

De forma análoga en el artículo 33.2 de la LOPDGDD, se establece que tendrá la consideración de responsable del tratamiento, y no la de encargado, quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del RGPD [5].

Propuesta Nro. 31: Añadir al final Artículo 72.
Obligaciones del encargado del tratamiento de datos personales.
(…)

13. Si un encargado del tratamiento infringe la presente Ley al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento

Artículo 29. Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.
El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

El artículo 29 del RGPD, ratifica el criterio anterior sobre las obligaciones del encargado.

6.5. Registro de las actividades de tratamiento

Artículo 30. Registro de las actividades de tratamiento
1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e)en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.
2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:
a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 90. Registro Nacional de Protección de Datos Personales: El responsable del tratamiento de datos personales deberá reportar a la Autoridad de Protección de Datos, lo siguiente
1. Identificación de la base de datos o del tratamiento;
2. El nombre, domicilio legal y datos de contactabilidad del responsable y encargado del tratamiento de datos personales;
3. Características y finalidad del tratamiento de datos personales;
4. Naturaleza de los datos personales tratados:
5. Identificación, nombre, domicilio legal y datos de contactabilidad de los destinatarios;
6. Modo de interrelacionar la información registrada,
7. Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada:
8 Requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9. Tiempo de conservación de los datos;
10. Transferencias internacionales:
11. Constancia de la existencia de códigos de conducta: y,
12. Constancia de disponibilidad de certificaciones, sellos y marcas de protección de datos personales:

Se obliga al responsable del tratamiento, y en su caso al encargado, a llevar un registro de las actividades de tratamiento que describa esas actividades y las medidas de seguridad aplicadas. El artículo determina que esas medidas serán establecidas en función al riesgo detectado, para lo cual se exige un análisis de riesgo previo al tratamiento [3]. La información que compone el registro debe ser descrito en algún cuerpo normativo, sin embargo, en el Proyecto no existe ningún articulado que defina el detalle descrito en el RGPD, por lo que podría detallarse posteriormente en el Reglamento General a Ley de Protección de Datos Personales o en su defecto en la normativa secundaria, que se genere por parte de la Autoridad a efectos de la ejecución del control de las actividades del responsable y del encargado.

El RGPD indica que el responsable debe llevar el registro, en el Proyecto de Ley además de esto supone que debe reportar el registro a la Autoridad de Control. En la definición de las condiciones de las empresas obligadas a llevar el registro, tanto del responsable como del encargado, el RGPD dirige a sus Estados Miembros que la organización cuente con más de 250 empleados. En Ecuador una pequeña y mediana empresa se encuentra definida por dos factores: número de empleados y el monto de sus ingresos brutos [13] de la siguiente manera:

- Microempresas: Ingresos menores a US$100.000. Trabajadores: entre 1 a 9 personas
- Pequeña empresa: Ingresos entre US$ 100.001 y US$ 1'000.000. Trabajadores: entre 10 a 49 personas
- Mediana empresa: Ingresos entre US$ 1'000.001 y US$ 5'000.000. Trabajadores: entre 50 a 199 personas

Por tanto, una recomendación para el siguiente nivel de normativa (Reglamento a la Ley) será definir esta obligación asimétrica para los diferentes tipos de organizaciones.

Artículo 31. Cooperación con la autoridad de control
El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

No está presente un artículo similar en el Proyecto de Ley.

7. Seguridad de los datos personales

7.1. Seguridad del tratamiento

Artículo 32. Seguridad del tratamiento
1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **el responsable y el encargado** del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4.El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del

responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 50. Seguridad de datos personales:
El responsable o encargado del tratamiento de datos personales, según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales.
El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.
El responsable o encargado del tratamiento de datos personales deberá demostrar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes:
1. Medidas de anonimización, encriptación, cifrado o codificación de datos personales:
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales de forma rápida en caso de incidentes: y.
3. Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.
Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares para medición y gestión de riesgos, así como para la Implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Nuevamente el Proyecto de Ley, difiere de forma importante con el RGPD: mientras el Reglamento Europeo define la obligación para la responsable y el encargado, el Proyecto menciona por tres ocasiones “el responsable o encargado”. En este caso, se considera una disolución de la responsabilidad, porque el responsable puede esperar que el encargado adopte las medidas de seguridad y viceversa. Por este motivo, en este aspecto, es recomendable apegarse estrictamente al modelo del RGPD, porque las medidas de seguridad deben mantenerse en todos los niveles, en las actividades del responsable y del encargado.

Propuesta Nro. 32. Modificar Artículo 50. Seguridad de datos personales.

El responsable y el encargado del tratamiento de datos personales, según sea el caso, deberán sujetarse al principio de seguridad (…)
El responsable y el encargado del tratamiento de datos personales, deberán implementar un proceso de verificación (…)
El responsable y el encargado del tratamiento de datos personales deberán demostrar que las medidas (…)

7.2. Notificación de una violación de la seguridad

Artículo 33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control
1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 55. Notificación de vulneración de seguridad: El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, dentro del término de tres (3) días a partir del conocimiento de dicha vulneración.
El encargado de tratamiento deberá notificar al responsable la vulneración de la seguridad de datos personales en un término no mayor a dos (2) días después de tener conocimiento de ella.
En caso de retraso del responsable o del encargado del tratamiento de datos personales en la notificación de vulneración de seguridad, sin que intermedie la debida justificación, se aplicarán las sanciones correspondientes, conforme a lo establecido en la presente ley.
En la notificación deberá constar lo siguiente:
1. La descripción de la naturaleza de la vulneración de la seguridad de los datos personales,
2. Las categorías y el número aproximado de titulares afectados;
3. Las categorías y el número aproximado de registros o campos de datos personales afectados;
4. El nombre y los datos de contacto del delegado de protección de datos, o a falta de este, de cualquier otro punto de contacto;

5. La descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales;
6. La descripción de las medidas adoptadas, implementadas o propuestas por el responsable para remediar la vulneración de la seguridad de los datos personales; y,
7. De ser el caso, las medidas adoptadas e implementadas para mitigar los posibles efectos negativos de la vulneración de la seguridad de datos personales.
Una vez tomado conocimiento de la vulneración de las seguridades de datos personales, el responsable deberá efectuar el **análisis de riesgo** sobre los derechos de libertad de sus titulares.
La notificación de las vulneraciones de seguridad de datos personales tendrá como objeto principal que la Autoridad de Protección de Datos Personales lleve un registro estadístico sobre vulneraciones e identificar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover nuevas regulaciones que busquen mejorar las seguridades exigibles a los responsables de tratamiento y otorgar seguridad jurídica en el tratamiento de datos personales.
La Autoridad de Protección de Datos Personales **sólo podrá sancionar al responsable o encargado** del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. En tal caso, la notificación oportuna de la violación por parte del responsable de tratamiento, tanto a la autoridad como al titular, así como las medidas de respuesta adoptadas, serán considerados como un atenuante de la infracción.
En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

El responsable debe notificar a la Autoridad de Control. El Proyecto de ley difiere en cuanto a que define un plazo para que el encargado notifique al responsable. Los plazos del RGPD son más flexibles: "*sin dilación indebida y, de ser posible, a más tardar 72 horas*" y "*la información se facilitará de manera gradual sin dilación indebida*". Para un control más efectivo, todos los plazos en el proyecto de ley se deberían establecer en el término de horas y en lugar de días.

En el proyecto de ley también se añaden aspectos que no necesariamente tienen relación directa con la actividad de notificación, como son: la acción subsiguiente que se adoptará en la Autoridad de Control con las notificaciones, esto es, que se sancionará al responsable o encargado, aspecto de corresponsabilidad que ha sido discutido anteriormente en el presente trabajo. Por último se establece que, una vez notificado, el responsable deberá realizar un análisis de riesgos, esto se considera un error de concepto, porque el análisis de riesgos se realiza antes de que se produzca un incidente de seguridad; lo que cabría en esa instancia es realizar un análisis del impacto sobre los datos personales a causa de la ocurrencia del evento.

Propuesta Nro. 33 Modificar Artículo 55.
(…)
Una vez tomado conocimiento de la vulneración de las seguridades de datos personales, el responsable deberá efectuar *el análisis del impacto* sobre los derechos de libertad de sus titulares.
(…)
La Autoridad de Protección de Datos Personales *podrá sancionar de acuerdo al régimen sancionatorio de la presente ley,* en tal caso, las notificaciones oportunas realizadas, serán consideradas como un atenuante de la infracción.

7.3. Comunicación de una violación de la seguridad al interesado

Artículo 34. Comunicación de una violación de la seguridad de los datos personales al interesado
1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).
3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:
a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.
4.Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Artículo 57. Notificación de vulneración de seguridad al titular: El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a su titular, cuando conlleve un riesgo a sus derechos de libertad, de forma inmediata o hasta dentro de un término de tres (3) días, contados a partir de tener conocimiento del riesgo.
No se deberá notificar al titular si se cumple alguna de las siguientes condiciones:
1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas, organizativas o de cualquier otra índole apropiadas, aplicadas a los datos personales afectados por la vulneración de su segundad;
2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que ya no se concrete el riesgo para los derechos de libertad del titular; y,
3. Cuando se requiera un esfuerzo desproporcionado, para lo cual se realizará una comunicación pública a través de cualquier medio, en la que se informe a los titulares.
La notificación al titular del dato contendrá 10 señalado en el artículo precedente
En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

Existe una alta coincidencia entre los dos artículos comparados. Sin embargo, en el Proyecto de Ley se ha omitido la posibilidad de que la Autoridad de Control, evalúe y a su criterio disponga al responsable la notificación a los titulares potencialmente afectados, este aspecto es muy importante, caso contrario, el responsable decidiría por su propia cuenta que una violación no comporta un alto riesgo, que sus medidas

de protección son suficientes, o que es un esfuerzo desproporcionado notificar a los titulares de los datos personales. Para eliminar esta subjetividad, es necesario que sea la Autoridad de Control quien defina si en realidad no cabe una notificación a los afectados. También será necesario añadir los elementos que deberá contener la notificación a los titulares, aspecto que se describe en el RGPD en el apartado 34.2., y en el artículo 55 del proyecto de ley.

Propuesta Nro. 34: Añadir al Artículo 57. Notificación de vulneración de seguridad al titular:
(…)

Cuando el responsable todavía no haya comunicado al titular la violación de la seguridad de los datos personales, la Autoridad de Protección de Datos Personales, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle al responsable que lo haga.
La comunicación al titular describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 55, numerales 4, 5, 6 y 7.

7.4. Evaluación de impacto

Artículo 35. Evaluación de impacto relativo a la protección de datos
1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.
4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.
5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.
6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63

si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.
7. La evaluación deberá incluir como mínimo:
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.
8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.
9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.
10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.
11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 54. Evaluación de impacto del tratamiento de datos personales: El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se ha identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleva un alto riesgo para los derechos y libertades del titular.
La evaluación de impacto del tratamiento de datos personales podrá analizar un conjunto de tratamientos equivalentes que conlleven altos riesgos similares.
La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales mencionado en el presente artículo.

El artículo relativo a la evaluación del impacto redactado en el Proyecto de Ley, difiere mucho del detalle plasmado en el RGPD. En el primero se presenta una síntesis que describe en qué condiciones se convierte en una obligación para el responsable del tratamiento, es por esto, que de forma mínima se debería agregar lo descrito en el apartado 3 del artículo 35 del RGPD. Aspecto importante constituye la elaboración de

perfiles puesto que el uso del perfil informático en la toma de decisiones que afecten a un individuo significará normalmente su discriminación en muchas de las actividades de la vida cotidiana [7].

Propuesta Nro. 35: Añadir al Artículo 54. Evaluación de impacto del tratamiento de datos personales.
(…)
La evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;
b) tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, o
c) observación sistemática a gran escala de una zona de acceso público.
La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

Artículos que constan en el Proyecto de Ley y no constan en el RGPD

Artículo 51. Medidas de seguridad en el ámbito del sector público: El mecanismo gubernamental de seguridad de la información incluirá las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.
El alcance de aplicación del mecanismo gubernamental de seguridad de la información, que incluya las disposiciones establecidas en el primer párrafo del presente artículo, abarcará a todos los miembros del sector público, conforme a lo detallado en el artículo 225 de la Constitución de la República del Ecuador.
Las instituciones mencionadas en el párrafo precedente podrán incorporar medidas adicionales a las establecidas en el mecanismo gubernamental de seguridad de la información, atendiendo a la naturaleza de sus atribuciones y funciones.

Al respecto, en Ecuador se ha definido el "*Esquema Gubernamental de Seguridad de la Información*" [14], que pretende ser el sistema de gestión de seguridad en las instituciones públicas y se basa en los estándares internacionales ISO 27001 e ISO 27002. El mismo define lo siguiente:

- Estructura organizacional de seguridad: Comité de Seguridad y Oficial de Seguridad.
- Sistema de Gestión de Seguridad de la Información: principios y beneficios.
- Proceso de mejora continua (PDCA) asociado al estándar ISO 27001.

El estándar ISO 27002 define en uno de sus controles de seguridad la protección de datos personales. Es en este Esquema Gubernamental que debe definirse el mecanismo gubernamental de seguridad, no cabe diferenciar en una Ley un apartado específico para el sector público. De considerarlo, se podría incluir como una disposición adicional al final de la Ley como se lo realiza en la LOPDGDD en su Disposición adicional primera relativa a las medidas de seguridad en el ámbito del sector público [3].

Propuesta Nro. 36: Eliminar el Artículo 51. Medidas de seguridad en el ámbito del sector público

Artículo 53. Análisis de riesgo y determinación de medidas de seguridad aplicables: Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de datos personales deberán utilizar una metodología que considere, entre otros:
l. Las particularidades del tratamiento;
2. Las particularidades de las partes involucradas, y,
3. El tipo y volumen de datos personales objeto del tratamiento.
Para determinar las medidas de seguridad, necesarias y adecuadas, se deberán tomar en cuenta, entre otros
l. Los resultados del análisis de riesgos, amenazas y vulnerabilidades:
2. La naturaleza de los datos personales:
3. Las características de las partes involucradas: y.
4. Los antecedentes de destrucción de datos personales, pérdida, alteración, divulgación o impedimento de acceso al titular a los mismos, sean éstas accidentales o intencionales. por acción u omisión, así como los de transferencia, comunicación, o acceso no autorizados o en exceso de autorización a dichos datos.
El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, Reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Aunque el RGPD no incluye un artículo especifico con el enunciado de análisis de riesgos, a lo largo de todo el documento (también en los considerandos), exige que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo. El tipo de análisis variará en función de [3]:
• Los tipos de tratamiento,
• La naturaleza de los datos,
• El número de interesados afectados,
• La cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Adicionalmente el artículo 53 del Proyecto de Ley se encuentra inmediatamente anterior al titulado “evaluación del impacto”, antes de realizar tal evaluación, las mejores prácticas de seguridad de la información establecen como paso previo desarrollar la actividad del análisis de riesgos. Por todos estos aspectos se considera adecuada la existencia del artículo 53.

Artículo 56. Acceso a datos personales para atención a emergencias e incidentes informáticos: Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de segundad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades durante el tiempo y alcance necesarios para, de forma exclusiva, su detección, análisis, protección y respuesta ante incidentes, así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

Es posible una base jurídica distinta al consentimiento por parte del titular al tratamiento de datos personales, en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información [3]. En este caso, son intereses legítimos los servicios conexos ofrecidos por, o accesibles a través de estos sistemas o redes por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de repuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad.

El artículo 56 del Proyecto de Ley permite el acceso a datos personales, a los siguientes actores:

- autoridades públicas competentes,
- equipos de respuesta de emergencias informáticas,
- equipos de respuesta a incidentes de segundad informática,
- centros de operaciones de seguridad,
- prestadores y proveedores de servicios de telecomunicaciones y
- proveedores de tecnología y servicios de seguridad, nacionales e internacionales

Sin embargo, es pertinente hacer aclaraciones puntuales que limiten este tipo de acceso:

- Los centros de operaciones de seguridad (SOC) son entidades dedicadas exclusivamente a la respuesta de incidentes informáticos.
- Los prestadores de servicios de telecomunicaciones es un grupo distinto al de los proveedores de servicios de comunicaciones electrónicas, porque los prestadores de telecomunicaciones pueden brindar servicios incluidos los de radiodifusión, servicios que no tienen relación con la seguridad de las redes informáticas.
- Los proveedores internacionales de servicios de seguridad no forman parte del ámbito de aplicación territorial.

Propuesta Nro. 37: Modificar Artículo 56. Acceso a datos personales para atención a emergencias e incidentes informáticos.

Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de segundad informática, los centros de operaciones de seguridad, los proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán acceder (…)

<u>Artículos que constan en el RGPD y no constan en el Proyecto de Ley</u>

Artículo 36. Consulta previa
1.El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.
(…)

Este mecanismo puede definirse posteriormente en el Reglamento a la Ley de Protección de Datos Personales.

7.5. Designación del delegado de protección de datos

Artículo 37. Designación del delegado de protección de datos
1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.
2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.
3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.
5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.
6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.
7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 58. Delegado de protección de datos personales: Se designará un delegado de protección de datos personales cuando:
1. El tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República,
2. Las actividades del responsable o encargado de tratamiento de datos personales requieran de un control permanente *y* sistematizado debido a su volumen, naturaleza, alcance y/o finalidades del tratamiento.
3. Se refiera a tratamientos de gran volumen de categorías especiales de datos; y.
4. El tratamiento se refiera a datos relacionados con la seguridad nacional y defensa del Estado no regulado por normativa especializada.

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones para la necesidad de contar con un Delegado de Protección de Datos Personales, así como emitir directrices para su designación.

La principal diferencia entre los dos artículos radica en las opciones del RGPD acerca de la designación de un único DPO para varias organizaciones. Otra diferencia se refiere a que en el proyecto de ley no se establece la obligación de comunicar a la Autoridad de control sobre a designación del delegado.

Propuesta Nro. 38: Añadir al final Artículo 58. Delegado de protección de datos personales
El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la Autoridad de Protección de Datos Personales.

7.6. Posición del delegado de protección de datos

Artículo 38. Posición del delegado de protección de datos
1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.
6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 59. Consideraciones especiales para el delegado de protección de datos personales: Para la ejecución de sus funciones como delegado de protección de datos personales, se deberá considerar lo siguiente:
1. Corresponde al responsable y al encargado garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna:
2. Es responsabilidad del responsable y del encargado facilitar el acceso a los datos personales y a las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones.

3. Corresponde al responsable y al encargado capacitar y actualizar los conocimientos del delegado de protección de datos personales en la materia, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales;
4. El responsable y el encargado no podrán destituir o sancionar al delegado de protección de datos personales por el desempeño de sus funciones;
5. El delegado de protección de datos personales mantendrá relación directa con el más alto nivel jerárquico del responsable o encargado;
6. El titular podrá contactar al delegado de protección de datos personales en relación al tratamiento de sus datos personales y al ejercicio de sus derechos:
7. El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones; y.
8. Siempre que no exista conflicto con sus responsabilidades establecidas en la presente ley, su
Reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado.

Concordancias:
El apartado 59.1 con el apartado 38.1: participación adecuada.
El apartado 59.2 con el apartado 38.2: respaldo en la funciones.
Los apartados 59.4 y 59.5 con el apartado 38.3: independencia en las funciones.
El apartado 59.6 con el apartado 38.4: contacto entre delegado e interesados.
El apartado 59.7 con el apartado 38.5: confidencialidad en el desempeño de funciones.
El apartado 59.8 con el apartado 38.6: desempeño de otras funciones.

Existe similitud en seis de los aspectos enumerados por el RGPD, a excepción del numeral 3 del Proyecto de Ley, relativo a que corresponde al responsable y al encargado capacitar y actualizar los conocimientos del delegado de protección de datos personales en la materia.

7.7. Funciones del delegado de protección de datos

Artículo 39. Funciones del delegado de protección de datos
1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:
a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; 60.2
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
d) cooperar con la autoridad de control;
e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Artículo 60. Funciones del delegado de protección de datos personales: El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:
1. Informar y asesorar al responsable y encargado del tratamiento de datos personales, así como al personal relacionado al tratamiento de datos personales, respecto a las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia,
2. Supervisar el cumplimiento de las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
3. Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, así como supervisar su aplicación; y,
4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad en relación a las cuestiones referentes al tratamiento.
La Autoridad de Protección de Datos Personales podrá definir otras funciones, atribuciones y responsabilidades para el delegado de protección de datos personales, atendiendo a la naturaleza de los datos de carácter personal, al ámbito, el contexto y finalidades del tratamiento.
En caso de incumplimiento de sus funciones, responderá administrativa, civil y penalmente

Concordancias:
El apartado 60.1 con el apartado 39.1a): asesorar al responsable o encargado.
El apartado 60.2 con el apartado 39.1b): supervisar el cumplimiento del Reglamento.
El apartado 60.4 con el apartado 39.1d): cooperar con la autoridad de control.
El apartado 60.4 con el apartado 39.1e): punto de contacto con la autoridad de control.
El párrafo sin numeración posterior al apartado 60.4 con el apartado 39.2: atención a los riesgos.

Existe similitud en los cuatros aspectos de las funciones definidos en el RGPD.

No obstante el proyecto de ley señala respecto al delegado: *"en caso de incumplimiento de sus funciones, responderá administrativa, civil y penalmente"*. Esto debería ser abordado desde la relación contractual con el responsable, y que no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. Entonces el delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado [5]; en tal virtud, el término "penal" no es pertinente en el ámbito de la ley de protección de datos.

Además en el Proyecto de Ley se presenta nuevamente el error de concepto del apartado 60.3, esto es realizar un análisis de riesgos, cuando respecto al tratamiento de los datos personales, al delegado únicamente le corresponde asesorar sobre la evaluación del impacto.

Propuesta Nro. 39: Modificar Artículo 60. Funciones del delegado de protección de datos personales
(…)
3. Asesorar en la evaluación de impacto y evaluación de medidas de seguridad, así como supervisar su aplicación; y,

(…)
Eliminar: En caso de incumplimiento de sus funciones, responderá administrativa, civil y penalmente

7.8. Códigos de conducta

Artículo 40. Códigos de conducta
1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.
2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:
(…)

Artículo 41. Supervisión de códigos de conducta aprobados
1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.
(…)

En el Proyecto de Ley no se han establecido artículos similares a los dos citados anteriormente del RGPD, no se define la existencia de organismos que tengan el nivel adecuado para la supervisión de códigos de conducta. A partir del artículo 61 del proyecto se menciona la posibilidad de adherirse a códigos denominados de "protección".

7.9. Certificación

Artículo 42. Certificación
1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.
2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros

instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.
3. La certificación será voluntaria y estará disponible a través de un proceso transparente.
4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.
5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.
6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.
7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.
8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 61. Aplicación del principio de responsabilidad proactiva: Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de protección, estándares, certificaciones, sellos y mejores prácticas para dar cumplimiento al principio de responsabilidad proactiva, sin que esto constituya eximente de la responsabilidad de cumplir con las disposiciones de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia.
La Autoridad de Protección de Datos Personales aprobará los contenidos de códigos de protección; evaluará, controlará, autorizará, sancionará y revocará, cuando sea procedente, las autorizaciones otorgadas a entidades certificadoras para su funcionamiento, así como evaluará, controlará y, de ser el caso, revocará las certificaciones y sellos otorgados por dichas entidades, y, además avalará estándares y mejores prácticas.

El objeto de los artículos es similar, esto es, respaldar el desempeño en materia de protección de datos personales con la adopción de forma voluntaria a códigos de conducta, estándares, certificaciones y sellos de protección. Se encuentra una diferencia respecto a que el RGPD promueve que las autoridades de control elaboren códigos de conducta como forma de contribuir a la correcta aplicación del Reglamento, mientras que en el Proyecto de Ley se otorgaría a la Autoridad de Control la capacidad de aprobación de los códigos y de revocar las autorizaciones a las entidades de certificación y las certificaciones que éstas emitan, es decir, tiene exclusivamente la competencia de control pero no la competencia de aportar con códigos tipo.

Tampoco se menciona en el Proyecto de Ley, que los códigos de conducta podrían promoverse por asociaciones u otros organismos que representen a categorías de responsables o encargados de tratamiento, por empresas o grupos de empresas, así como por las Administraciones Públicas y las entidades pertenecientes al sector público tal como se establece en el apartado 40.2 del RGPD.

A fin de aportar claridad al Proyecto de Ley, es importante expresar que la Autoridad de Control, tiene competencia respecto a la autorización del funcionamiento de una entidad certificadora y no únicamente a las certificaciones que éstas emitan, y separar con las otras funciones relacionadas a la gestión de la responsabilidad proactiva.

Propuesta Nro. 40 Modificar segundo párrafo Artículo 61. Aplicación del principio de responsabilidad proactiva.
(…)
Los códigos de protección tienen carácter voluntario, por lo que únicamente obligan a quienes se han comprometido a aplicarlos.
La Autoridad de Protección de Datos Personales tendrá competencia para:
- Aprobar los contenidos de códigos de protección*;*
- *Autorizar el funcionamiento de las entidades certificadoras,*
- Evaluar, controlar, autorizar, sancionar y revocar, cuando sea procedente, las certificaciones y sellos otorgados por las entidades*;*
- Avalar estándares y mejores prácticas*.*

7.10. Organismo de certificación

Artículo 43. Organismo de certificación
1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:
a) la autoridad de control que sea competente en virtud del artículo 55 o 56;
b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.o 765/2008 del Parlamento Europeo y del Consejo (1) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.
2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:
a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;
b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;
c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;
d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.
3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los criterios aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.o 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.
4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.
5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.
6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se a refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité. El Comité archivará en un registro todos los mecanismos de certificación y sellos de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.
7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.
8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.
9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. Atribuciones de las Entidades de Certificación: En materia de protección de datos personales, las Entidades de Certificación, podrán:
1. Emitir certificaciones de cumplimiento de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
2. Emitir sellos de protección de datos personales;
3. Llevar a cabo auditorías de protección de datos personales, y,
4. Certificar los procesos de transferencias internacionales de datos personales.
Los resultados de las auditorías podrán ser considerados como elementos probatorios dentro de los procesos sancionatorios.

Artículo 63. Reconocimiento y revocatoria como Entidad Certificadora: La Autoridad de Protección de Datos Personales emitirá las directrices para la constitución y autorización de funcionamiento de las Entidades Certificadoras, y para su evaluación continua y permanente.
La Autoridad de Protección de Datos Personales, mediante resolución motivada, podrá revocar, de ser el caso, la autorización de funcionamiento como Entidad Certificadora en cualquier momento

Se entrega a la Autoridad de Control la responsabilidad de emitir normativa secundaria para autorizar a las entidades, pero además se incluye el término "directrices para la constitución", atribución que no correspondería a una competencia de una Autoridad de Protección de datos sino a la autoridad de control de compañías.
El Proyecto de Ley carece de una definición sobre la jerarquía adoptada durante el proceso de certificación y que se distinga con el proceso de acreditación de las entidades; sin embargo, debido a que en el Ecuador no existe un organismo nacional de acreditación, le correspondería a la misma Autoridad de Control de protección de datos la competencia de acreditar a las Entidades certificadoras relacionadas.

Propuesta Nro. 41. Modificar Artículo 63. Reconocimiento y revocatoria como Entidad Certificadora.

La Autoridad de Protección de Datos Personales constituye en el país el organismo de acreditación de las Entidades Certificadoras relacionadas a la protección de datos personales, para el efecto emitirá las directrices para la autorización de su funcionamiento y evaluación continua y permanente.
La Autoridad de Protección de Datos Personales, mediante resolución motivada, podrá revocar, de ser el caso, la autorización de funcionamiento como Entidad Certificadora en cualquier momento.
Los organismos de certificación comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

8. Transferencias internacionales

8.1. Principio general

Artículo 44. Principio general de las transferencias
Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 64. Transferencia o comunicación internacional de datos personales: La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo

previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales

Existe plena concordancia entre los dos artículos.

8.2. Transferencias basadas en adecuación

Artículo 45. Transferencias basadas en una decisión de adecuación
1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.
2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:
a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;
b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.
3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. **El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años**, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.
4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las

decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.
5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.
6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.
7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.
8. La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

Artículo 65. Criterios para declarar el nivel adecuado de protección: Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la cual se verificará la existencia de los siguientes presupuestos:
l. Que cuente con normativa que promueva y garantice el ejercicio de derechos fundamentales y libertades individuales;
2. Que cuente con una autoridad estatal independiente que garantice y promueva la efectiva tutela del derecho a la protección de datos personales;
3. Que cuente con normativa especializada en materia de protección de datos personales;
4. Que sea parte de Acuerdos o instrumentos internacionales, vinculantes ratificados por un tercer país u organización que generen obligaciones respecto al tratamiento y trasferencia o comunicación de datos personales, siempre que estos establezcan un estándar igualo mayor de protección en favor del titular, más allá de su origen o nacionalidad, y,
5. Que posea legislación específica en materia segundad nacional y defensa del Estado, que establezca mecanismos de control y verificación del acceso de las autoridades públicas a los datos personales de sus ciudadanos.
La resolución de nivel adecuado de protección **deberá contemplar mecanismos de revisión periódica, al menos cada cinco años**, para garantizar el derecho a la protección de datos personales. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países

Artículo 66. Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección.

Por principio general se podrán transferir o comunicar datos personales a países u organizaciones que brinden niveles adecuados de protección, conforme a los criterios establecidos en el artículo precedente.

Concordancias:
El artículo 66, con el apartado 45.1: transferencias con nivel de protección adecuado.
Los apartados 65.1, 65.3 y 65.5 con el apartado 45.2a): principales criterios para evaluar el nivel de protección.
El apartado 65.2 con el apartado 45.2b): existencia de autoridad de control en el tercer país.
El apartado 65.4 con el apartado 45.2c): compromisos internacionales con el tercer país.

La primera diferencia formal consiste en las funciones del Comité de la Unión Europea definidas en el RGPD, que son asumidas por la Autoridad de Protección de Datos Personales en el proyecto de ley. La segunda diferencia formal consiste en que el artículo 45.3 del RGPD establece una revisión periódica cada 4 años del acto de ejecución, mientras que en el Proyecto de Ley se establece una revisión cada 5 años de la resolución motivada.

8.3. Transferencias mediante garantías adecuadas

Artículo 46. Transferencias mediante garantías adecuadas
1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
b) normas corporativas vinculantes de conformidad con el artículo 47;
c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;
e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:
a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.
4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.
5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 67. Transferencia o comunicación mediante garantías adecuadas. Este mecanismo de transferencia o comunicación transfronteriza de datos personales opera cuando no existe una resolución de nivel adecuado de protección, en su lugar el responsable o encargado del tratamiento de datos personales deberá tomar medidas para compensar la falta de protección de datos en un tercer país u organización mediante garantías adecuadas para el titular, debiendo cumplir al menos con las siguientes:
l. Observancia de principios, derechos y obligaciones en el tratamiento de datos personales siempre que estos cumplan con un estándar igualo mayor de protección;
2. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,
3. El derecho a solicitar la reparación integral, de ser el caso
Para la consecución de este mecanismo se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables del tratamiento de datos personales tales como: normas corporativas vinculantes, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas, códigos de protección, mecanismos de certificación, sellos de protección de datos personales aprobados
Corresponde a la Autoridad de Protección de Datos Personales dictar el contenido de las cláusulas estándar de protección de datos, así como la verificación de cláusulas o garantías adicionales o específicas acordadas entre las partes.
La Autoridad de Protección de Datos Personales aprobará códigos de protección, mecanismos de certificación y sellos de protección de datos personales.
Para el cumplimiento de lo previsto en el presente artículo, se considerarán los derechos, garantías y principios de la presente ley, como requisitos y condiciones mínimas para la transferencia o comunicación internacional.

El artículo 46 del RGPD es muy descriptivo sobre los casos y condiciones que deben cumplirse para las transferencias mediante garantías adecuadas: seis garantías adecuadas sin autorización de la Autoridad de Control (apartado 46.2) y dos garantías adecuadas con la autorización de la Autoridad de Control (apartado 46.3). Por su parte, el Proyecto de Ley en el primer párrafo sin numeración cita seis garantías: normas corporativas vinculantes; cláusulas estándar de protección de datos; cláusulas o garantías adicionales o específicas; códigos de protección; mecanismos de certificación; y sellos de protección de datos personales aprobados; sin embargo, no se indica en el proyecto que alguna de esas garantías requieran autorización de la Autoridad de Control, en este sentido existe coincidencia con el apartado 46.2 del RGPD, y se excluye las garantías especificadas en 46.3 del RGPD, las cuales deberían incluirse.

La frase: “cláusulas o garantías adicionales o específicas” es un texto genérico al que debería limitarse según lo que corresponde a la Autoridad de Control autorizar, y no únicamente corresponde verificar.

Propuesta Nro. 42. Modificar Artículo 67. Transferencia o comunicación mediante garantías adecuadas.
(…)
Para la consecución de este mecanismo, *sin que medie la autorización de la Autoridad de Protección de Datos Personales*, se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables del tratamiento de datos personales tales como: normas corporativas vinculantes, cláusulas estándar de protección de datos, códigos de protección, mecanismos de certificación y sellos de protección de datos personales aprobados; *y, previa autorización de la Autoridad de Protección de Datos Personales,* para el aporte de garantías constantes en cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.
Corresponde a la Autoridad de Protección de Datos Personales *dictar el contenido de las cláusulas estándar de protección de datos.*
La Autoridad de Protección de Datos Personales aprobará códigos de protección, mecanismos de certificación y sellos de protección de datos personales, conforme lo establece el artículo 61 de la presente Ley.
(…)

8.4. Transferencias basadas en Normas corporativas vinculantes

Artículo 47. Normas corporativas vinculantes
1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:
a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;
b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y
c) cumplan los requisitos establecidos en el apartado 2.
2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:
a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, **el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión**;
c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;
d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los **derechos de los interesados** en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el **derecho a obtener una reparación**, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;
f) la **aceptación por parte del responsable o del encargado** del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
g) la **forma en que se facilita a los interesados la información** sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;
h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;
i) los procedimientos de reclamación;
j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;
k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;
l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);
m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y
n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.
3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente

artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 68. Normas corporativas vinculantes: Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, en las cuales, para su aprobación, deberán cumplir las siguientes condiciones.
l. **Ser de obligatorio cumplimiento** para el responsable de tratamiento, la totalidad del grupo empresarial al que ésta pertenezca, sus empresas asociadas y cualquier otra empresa a la que eventualmente transfieran datos personales;
2. **Brindar a los titulares los mecanismos** adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales, observando las disposiciones constantes en la presente ley;
3. Incluir una enunciación detallada de **las empresas filiales** que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además se incluirá **la estructura y los datos** de contacto del grupo empresarial o joint venture dedicadas a una actividad económica conjunta y de cada uno de sus miembros**;**
4. Incluir el detalle de las **empresas encargadas del tratamiento** de datos personales, las categorías de datos personales a ser utilizados, así como el tipo de **tratamiento** a realizarse y su **finalidad**;
5. Enunciar de forma expresa el **carácter jurídicamente vinculante** de tales normas a nivel nacional e internacional;
6. Observar en su contenido todas las disposiciones de la presente ley referentes a **principios** de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes**;**
7. Contener la **aceptación por parte del responsable o del encargado** del tratamiento de los datos personales o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si éste demuestra que el acto que originó los daños y perjuicios no le es imputable.
8. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes y sus efectos jurídicos;
9. Incluir las **funciones de todo delegado de protección** de datos designado o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control, así como los mecanismos y procesos de supervisión y tramitación de reclamaciones,
10. Detallar los procesos o procedimientos en vía administrativa o judicial que le asistan;
11. Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirá auditorías continuas de protección de datos y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán de acceso público, debidamente publicados y se pondrán a disposición de la Autoridad de Protección de Datos Personales en la periodicidad establecida en el reglamento a la presente ley;
12. Incluir los mecanismos para cooperar de forma coordinada con la Autoridad de Protección de Datos Personales y el responsable del tratamiento de los datos personales; y.
13. Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato *y* los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.
Cualquier cambio a ser realizado a estas normas deberá ser previamente aprobado por la Autoridad de Protección de Datos Personales y notificado al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud de aprobación.

Concordancias:
El apartado 68.3 con el apartado 47.2a): datos de contacto del grupo empresarial.
El apartado 68.4 con el apartado 47.2b): tipo de tratamientos y de interesados afectados.
El apartado 68.5 con el apartado 47.2c): carácter vinculante.
El apartado 68.6 con el apartado 47.2d): principios generales de protección de datos.
El apartado 68.7 con el apartado 47.2f): aceptación del responsable o del encargado.
El apartado 68.8 con el apartado 47.2g): forma de informar al interesado.
El apartado 68.9 con el apartado 47.2h): funciones del delegado.
El apartado 68.10 con el apartado 47.2i): procedimientos de reclamación.
El apartado 68.11 con el apartado 47.2j): mecanismos de verificación de cumplimiento.
El apartado 68.12 con el apartado 47.2l): mecanismo de cooperación con la autoridad de control.
El apartado 68.13 con el apartado 47.2n): protección de datos del personal.

Las normas corporativas vinculantes (Binding Corporate Rules), constituyen un instrumento que los grupos multinacionales que pueden hacer valer ante las autoridades de protección de datos, para garantizar la legalidad de las operaciones de transferencia de datos en su organización, independientemente de que el país de destino garantice o no un “adecuado nivel de protección” [3].

En los dos artículos comparados, el fin es el mismo, la Autoridad de control aprueba las normas corporativas vinculantes que presenten las organizaciones. En el Proyecto de Ley, se utiliza el término “join venture”, siendo el Ecuador un país con idioma oficial el español es recomendable se utilice la frase “unión de empresas dedicadas a una actividad económica conjunta” tal como se lo hace en el RGPD.
No aplica la intervención de la Comisión como en la Unión Europea, por la falta actual de un organismo análogo en el ámbito regional.

Propuesta Nro. 43. Modificar Artículo 68. Normas corporativas vinculantes.

Donde dice: “join venture”
Reemplazar por: “unión de empresas dedicadas a una actividad económica conjunta”

Artículo 48. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión
Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

No aplica en el Proyecto de Ley porque existe un distinto ámbito de aplicación territorial.

8.5. Transferencias excepciones para situaciones específicas

Artículo 49. Excepciones para situaciones específicas
1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:
a) el interesado haya dado explícitamente su **consentimiento** a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
b) la transferencia sea necesaria para la ejecución de un **contrato entre el interesado y el responsable** del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
c) la transferencia sea necesaria para la celebración o ejecución de un **contrato, en interés del interesado**, entre el responsable del tratamiento y otra persona física o jurídica;
d) la transferencia sea necesaria por razones importantes de **interés público**;
e) la transferencia sea necesaria para la formulación, el ejercicio o la **defensa de reclamaciones**;
f) la transferencia sea necesaria para proteger los **intereses vitales** del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar **información al público** y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.
Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo **si no es repetitiva**, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.
2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), **no abarcará la totalidad de los datos personales ni categorías enteras** de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte

de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.
3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las **actividades llevadas a cabo por las autoridades públicas** en el ejercicio de sus poderes públicos.
4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.
6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 69. Casos excepcionales de transferencias o comunicaciones internacionales: En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, **la Autoridad de Protección de Datos Personales podrá autorizar** transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:
1. A países u organismos internacionales que brinden garantías adecuadas para la protección de datos personales sin que necesariamente exista una ley específica o Autoridad de Protección de Datos Personales, para lo cual será necesaria la suscripción de un convenio o **tratado internacional**;
2. Cuando los datos personales sean requeridos para el cumplimiento de **competencias institucionales**, de conformidad con la normativa aplicable;
3. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de las finalidades del tratamiento y posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas;
4. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una **obligación legal o regulatoria**;
5. Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de una obligación **contractual entre el titular y el responsable** del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;
6. Cuando la transferencia internacional de datos personales sea necesaria para la celebración o ejecución de un contrato, en interés del titular entre el responsable del tratamiento de datos personales y otra persona natural o Jurídica;
7. Cuando la transferencia sea necesaria por razones de interés público;
8. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional.
9. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones**;**
10. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;
11. Transferencias bancarias y bursátiles;

12. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos, y.
13. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento

En el párrafo no numerado del artículo 49 del RGPD se introduce la posibilidad de realizar una transferencia internacional basada en el interés legítimo imperioso perseguido por el responsable. Para que sea posible la transferencia no deberá ser repetitiva, deberá afectar solo a un número limitado de interesados, deberá ser necesaria para conseguir los intereses legítimos imperiosos del responsable y no deberán prevalecer sobre los derechos y libertades del interesado [3].

Concordancias:
El apartado 69.3 con el apartado 49.1a): consentimiento.
El apartado 69.5 con el apartado 49.1b): contrato entre el interesado y el responsable.
El apartado 69.6 con el apartado 49.1c): contrato, en interés del interesado.
El apartado 69.7 con el apartado 49.1d): interés público.
El apartado 69.12 con el apartado 49.1e): defensa de reclamaciones.
El apartado 69.13 con el apartado 49.1f): intereses vitales.

No obstante, se verifican varias diferencias. La primera se refiere a que en el Proyecto de Ley, la Autoridad de Protección de Datos Personales deberá autorizar las transferencias excepcionales, mientras que en el RGPD, cuando se cumplen las condiciones del apartado 49.1, no se requiere autorización, sino únicamente que se informe a la Autoridad de Control.

Además en el Proyecto de Ley se contemplan casos adicionales, que no constan en el RGPD, y que permitirían una transferencia internacional basada en:

- competencias institucionales;
- obligación legal o regulatoria;
- convenio o tratado internacional;
- colaboración judicial internacional;
- cooperación dentro de la investigación de infracciones;
- cooperación internacional entre Estados; y,
- transferencias bancarias y bursátiles.

Respecto a las competencias institucionales y la existencia de una obligación legal o regulatoria, esto no se encuentra delimitado, por lo que implicaría un alto riesgo, en el caso que los responsables abusen al realizar transferencias con ésta condición. En relación a los convenios, colaboración, y cooperación internacional, esto supliría en parte la diferencia del ámbito de aplicación territorial de la Ley. Finalmente, se destaca que en el proyecto de ley la Autoridad de Control tendría una carga operativa alta para autorizar todas las transferencias internacionales de datos personales cuando éstas se refieran a transferencias bancarias y bursátiles, este último caso podría encasillarse en las normas corporativas vinculantes.

Artículo 50. Cooperación internacional en el ámbito de la protección de datos personales
En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;
b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;
c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;
d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

No aplicable en el ámbito de aplicación territorial.

Artículo del Proyecto de Ley no presente en el RGPD

Artículo 70. Control continuo: La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.
En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.
La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente actualizado, una lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales.

El artículo 70 presente en el Proyecto de Ley se encuentra relacionado con el artículo 65, referido a los criterios para declarar el nivel adecuado de protección, porque la evaluación implica el control continuo sobre el nivel de protección de datos de otros países.

9. Autoridad de control

9.1. Autoridad de control

Artículo 51. Autoridad de control
1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.
3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.
4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. Independencia
1. Cada autoridad de control actuará con **total independencia en el desempeño de sus funciones** y en el ejercicio de sus poderes de conformidad con el presente Reglamento.
2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.
3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.
4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.
5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.
6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 88. Autoridad de Protección de Datos Personales. La Autoridad de Protección de Datos Personales será una entidad de derecho público **dependiente de la Función Ejecutiva** con personería jurídica y gozará de autonomía administrativa y financiera.

Posiblemente la mayor diferencia entre el RGPD y el Proyecto de Ley se encuentra en la real y efectiva independencia de la Autoridad de Control. Esto fue mencionado anteriormente como una importante contradicción con los principios enunciados en el mismo Proyecto en los que se establece la independencia del control, pero en el artículo 88 señala que dicha autoridad sería dependiente del poder ejecutivo, lo cual hace improbable que se cumpla dicho principio.

Por ejemplo en Argentina, una vez promulgada la Ley 25.326 se crearía una autoridad con la denominación de Dirección Nacional de Protección de Datos Personales, sin embargo el poder Ejecutivo, realizó un veto parcial en ese momento, retirando a esa institución la autonomía e independencia, y de esa forma se limitó la función de velar por el cumplimiento de la ley, en forma imparcial e independiente de los organismos gubernamentales [19].

En el Estado ecuatoriano, la Constitución de la República establece que los organismos de control, independientes y autónomos, serán denominados Superintendencias, con este principio el último organismo de control creado al amparo de la Ley Orgánica de Regulación y Control del Poder de Mercado fue la Superintendencia de Control del Poder del Mercado. En materia de protección de datos personales, para una plena independencia cabe la creación de la Superintendencia de Protección de Datos.

Propuesta Nro. 43. Modificar Artículo 88.- Superintendencia de Protección de Datos.

*Créase la Superintendencia de Protección de Datos, misma que pertenece a la Función de Transparencia y Control Social, como un organismo técnico de control, con capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, patrimonio propio y autonomía administrativa, presupuestaria y organizativa; la que contará con amplias atribuciones para hacer cumplir todo lo dispuesto en la presente Ley. Su domicilio será la ciudad de Quito, sin perjuicio de las oficinas que pueda establecer el Superintendente en otros lugares del país***.**

9.2. Condiciones generales aplicables a la autoridad de control

Artículo 53. Condiciones generales aplicables a los miembros de la autoridad de control
1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por: — su Parlamento, — su Gobierno, — su Jefe de Estado, o — un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.
2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesaria para el cumplimiento de sus funciones y el ejercicio de sus poderes.
3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.
4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. Normas relativas al establecimiento de la autoridad de control
1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:
a) el establecimiento de cada autoridad de control;
b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;
c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;
d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;
e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.
2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Al establecer en primera instancia que la Autoridad de control de protección de datos es dependiente de la Función Ejecutiva, su nominación sería exclusiva por el Presidente de la República, por tanto el artículo 53 del RGPD no tiene un similar en el Proyecto de Ley. En el caso de crearse la Superintendencia de Protección de Datos y que tenga total independencia, se requerirá del articulado necesario para definir la forma y el procedimiento para el establecimiento de la Autoridad. Este procedimiento debe seguir el modelo de los lineamientos del RGPD apartado 54.1 y basarse en los términos establecidos en el artículo 213 de la Constitución del Ecuador; esto es, que los organismos de control independientes deben pertenecer a la Función de Transparencia de Control Social y los Superintendentes serán nombrados por el Consejo de Participación Ciudadana y Control Social de una terna que envía el Presidente de la República, conformada con criterios de especialidad y méritos y sujeta a escrutinio público y derecho de impugnación ciudadana [15].

Propuesta Nro. 44. Agregar Artículo 89. Del Superintendente

El Superintendente es la máxima autoridad administrativa, resolutiva y sancionadora, y le corresponde la representación legal, judicial y extrajudicial de la Superintendencia de Protección de Datos.

Propuesta Nro. 45. Agregar Artículo 90.- Designación del Superintendente de Protección de Datos

El Superintendente de Protección de Datos será nombrado por el Consejo de Participación Ciudadana y Control Social, de una terna enviada por el Presidente de la República para tal efecto, en la forma y con los requisitos previstos en la Constitución de la República y la ley.
El Superintendente desempeñará sus funciones por cinco años y podrá ser reelegido por una sola vez.
Para ser designado Superintendente de Protección de Datos, se requiere ser ecuatoriano, estar en ejercicio de los derechos de participación, tener título académico de cuarto nivel en materias afines a la competencia profesional, y experiencia particular en materia de protección de datos.

9.3. Competencia

Artículo 55. Competencia

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.
2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.
3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Propuesta Nro. 46. Agregar nuevo Artículo 91. Competencia de la Superintendencia de Protección de Datos

Corresponde a la Superintendencia de Protección de Datos supervisar la aplicación de ésta ley; ejercer las funciones, atribuciones y facultades establecidas en el artículo 92; y las funciones que le atribuyan otras leyes.

Artículo 56. Competencia de la autoridad de control principal

No tiene similar porque en el Proyecto de Ley se define únicamente la existencia de una Autoridad de Control.

9.4. Funciones

Artículo 57. Funciones
1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:
a) **controlar** la aplicación del presente **Reglamento** y hacerlo aplicar;
b) promover la **sensibilización** del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;
c) **asesorar**, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;
d) promover la **sensibilización** de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;
e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;
f) tratar las **reclamaciones** presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;
g) **cooperar**, en particular compartiendo información, con otras **autoridades de control** y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo **investigaciones** sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;
i) hacer un **seguimiento de cambios** que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;
j) adoptar las **cláusulas contractuales tipo** a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);
k) elaborar y mantener una **lista relativa al requisito de la evaluación de impacto** relativa a la protección de datos, en virtud del artículo 35, apartado 4;
l) ofrecer **asesoramiento** sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2
m) alentar la elaboración de **códigos de conducta** con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;
n) fomentar la creación de **mecanismos de certificación** de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;
o) llevar a cabo, si procede, una **revisión periódica de las certificaciones** expedidas en virtud del artículo 42, apartado 7;
p) elaborar y publicar los **criterios para la acreditación** de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;
q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;
r) autorizar las **cláusulas contractuales** y disposiciones a que se refiere el artículo 46, apartado 3;
s) aprobar **normas corporativas vinculantes** de conformidad con lo dispuesto en el artículo 47;
t) contribuir a las actividades del **Comité**;
u) llevar **registros internos de las infracciones** del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y
v) desempeñar cualquier otra función relacionada con la protección de los datos personales.
2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un **formulario de presentación de reclamaciones** que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.
3. El desempeño de las funciones de cada autoridad de control será **gratuito** para el interesado y, en su caso, para el delegado de protección de datos.
4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su **carácter repetitivo**, la autoridad de control podrá establecer una **tasa razonable** basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

9.5. Poderes

Artículo 58. Poderes
1. Cada autoridad de control dispondrá de todos los **poderes de investigación** indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten **cualquier información** que requiera para el desempeño de sus funciones;
b) llevar a cabo investigaciones en forma de **auditorías** de protección de datos;
c) llevar a cabo una **revisión de las certificaciones** expedidas en virtud del artículo 42, apartado 7;
d) **notificar** al responsable o al encargado del tratamiento las presuntas **infracciones** del presente Reglamento;
e) obtener del responsable y del encargado del tratamiento el **acceso a todos los datos personales** y a toda la información necesaria para el ejercicio de sus funciones;
f) obtener el **acceso a todos los locales del responsable** y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.
2. Cada autoridad de control dispondrá de todos los siguientes **poderes correctivos** indicados a continuación:
a) **sancionar** a todo responsable o encargado del tratamiento **con una advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;
b) **sancionar** a todo responsable o encargado del tratamiento **con apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
c) **ordenar** al responsable o encargado del tratamiento que **atiendan las solicitudes** de ejercicio de los derechos del interesado en virtud del presente Reglamento;
d) **ordenar** al responsable o encargado del tratamiento que las operaciones de **tratamiento se ajusten** a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
e) **ordenar** al responsable del tratamiento que **comunique al interesado las violaciones** de la seguridad de los datos personales;
f) **imponer** una **limitación** temporal o definitiva del tratamiento, incluida su prohibición;
g) **ordenar la rectificación o supresión de datos personales** o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;
h) **retirar una certificación** u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;
i) **imponer una multa administrativa** con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
j) **ordenar la suspensión de los flujos de datos** hacia un destinatario situado en un tercer país o hacia una organización internacional.
3. Cada autoridad de control dispondrá de todos los **poderes de autorización y consultivos** indicados a continuación:
a) **asesorar al responsable** del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;
b) **emitir**, por iniciativa propia o previa solicitud, **dictámenes** destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) **autorizar el tratamiento** a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;
d) emitir un dictamen y **aprobar proyectos de códigos de conducta** de conformidad con lo dispuesto en el artículo 40, apartado 5;
e) **acreditar los organismos de certificación** con arreglo al artículo 43;
f) **expedir certificaciones** y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;
g) **adoptar las cláusulas tipo de protección** de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);
h) **autorizar las cláusulas contractuales** indicadas en el artículo 46, apartado 3, letra a);
i) **autorizar los acuerdos administrativos** contemplados en el artículo 46, apartado 3, letra b);
j) **aprobar normas corporativas vinculantes** de conformidad con lo dispuesto en el artículo 47.
4.El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.
5. Cada Estado miembro dispondrá por ley **que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones** del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.
6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 89. Funciones, atribuciones y facultades:
Corresponden a la Autoridad de Protección de Datos Personales las siguientes funciones, atribuciones y facultades:
1. Ejercer la supervisión, **control** y evaluación de las actividades efectuadas por el **responsable y encargado** del tratamiento de datos personales y de las **entidades** certificadoras, de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;
2. **Conocer** sobre los **proyectos de normas** de carácter general o técnico que se desarrollen en materia de protección de datos personales;
3. **Emitir normativa** general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales.
4. Promover proyectos de ley o reformas en materia de protección de datos personales;
5. **Autorizar** y revocar la autorización de funcionamiento de **entidades** certificadoras, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
6. Revisar, **aprobar**, rechazar, revocar y exigir la modificación de **códigos de protección**, mecanismos de certificación o sellos de protección de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
7. **Revocar las certificacio**nes o sellos de protección en materia de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad *y* elaborar el modelo de gestión correspondiente.

8. Promover una **coordinación** adecuada y eficaz con entidades de certificación o agentes privados encargados de la rendición de cuentas, y participar en i**niciativas internacionale**s y regionales para la protección de la protección de los datos personales;
9. Dictar las **cláusulas estándar de protección** de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas,
10. Conocer, sustanciar y **resolver los reclamos** interpuestos por el titular o aquellos iniciados de oficio; así como aplicar las **sanciones** correspondientes,
11. Atender consultas en materia de protección de datos personales;
12. Promover e **incentivar el ejercicio del derecho** a la protección de datos personales.
13. Ejercer el **control** y emitir las resoluciones de autorización para la **transferencia** internacional de datos;
14. **Coordinar** con otros organismos del sector público y privado los esfuerzos para formular y aplicar planes y **políticas** destinados a fortalecer la protección de datos personales;
15. Ejercer la **representación internacional** en materia de protección de datos personales;
16. Coordinar, promover y ejecutar **programas de cooperación** con organismos internacionales análogos en materia de protección de datos personales, así como con unidades nacionales relacionadas, dentro del marco de sus competencias; y ejecutar acciones conjuntas a través de convenios de cooperación nacional o internacional;
17. Prestar **asistencia** en asuntos relacionados con la protección de datos personales a petición de un organismo nacional o internacional, de una entidad pública o privada:
18. Emitir **directrices** para el diseño y contenido de la **política** de tratamiento de datos personales;
19. Establecer **directrices** para el análisis, evaluación y selección de **medidas de seguridad** de los datos personales:
20. Llevar un **registro estadístico sobre vulneraciones** a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;
21. **Solicitar información** sobre su gestión a **responsables, encargados y entidades** de certificación para el cumplimiento de sus funciones de control y demás atribuciones establecidas en la presente ley;
22. **Realizar o delegar auditorías** técnicas al tratamiento de datos personales de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales; 58.1.b
23. Solicitar y recabar información para el análisis *y* elaboración de **estudios** en materia de protección de datos personales;
24. Publicar periódicamente una **guía de la normativa** relativa a la protección de datos personales;
25. Ejercer la **potestad sancionadora** respecto de responsables, encargados, terceros y entidades de certificación, conforme a lo establecido en la presente ley*;*
26. Crear, dirigir y administrar el **Registro Nacional** de Protección de Datos Personales, así como, coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;
27. Promover la **concientización** en las personas y la compresión de los riesgos, normas, garantías y derechos en relación con el tratamiento *y* uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria, tales como niñas, niños y adolescentes;
28. **Compartir con organismos internacionales** análogos en materia de protección de datos personales, así como con entidades nacionales e internacionales de control o fiscalización de índole administrativa o judicial (i) Informes, (ii) información; o (iii) datos personales relacionados a procesos de investigación, en el marco de sus competencias y de conformidad con la normativa aplicable, sin que dicha transferencia constituya una

vulneración al principio de confidencialidad al constituir parte de la cadena de custodia, con la finalidad exclusiva de realizar el análisis, investigación y toma de acciones legales, judiciales y las demás que fueren pertinentes, pudiendo ser además utilizada como instrumento probatorio;
29. Controlar y supervisar el ejercicio del derecho a la protección de datos personales dentro del tratamiento de datos llevado a cabo a través del **Sistema Nacional de Registros Públicos**, y,
30. Las demás atribuciones establecidas en la normativa vigente.

Concordancias de Funciones:
El apartado 89.27 con el apartado 57.1b): sensibilización del público.
El apartado 89.17 con el apartado 57.1c): asesorar al Parlamento y al Gobierno.
El apartado 89.27 con el apartado 57.1d): sensibilización de los responsables y encargados.
El apartado 89.11 con el apartado 57.1e): facilitar información a los interesados.
El apartado 89.10 con el apartado 57.1f): atender reclamaciones.
El apartado 89.14 con el apartado 57.1g): cooperar con autoridades de control.
El apartado 89.9 con el apartado 57.1j): adoptar las cláusulas contractuales tipo.
El apartado 89.6 con el apartado 57.1m): códigos de conducta.
El apartado 89.6 con el apartado 57.1n): mecanismos de certificación.
El apartado 89.5 con el apartado 57.1p): criterios para la acreditación.
El apartado 89.5 con el apartado 57.1q): efectuar la acreditación.

Concordancias de Poderes:
Los apartados 89.1 y 89.21 con el apartado 58.1a): ordenar cualquier información.
El apartado 89.22 con el apartado 58.1b): llevar auditorías.
El apartado 89.25 con el apartado 58.1d): notificar infracciones.
El apartado 89.1 con el apartado 58.1e): acceso a todos los datos personales.
El apartado 89.25 con el apartado 58.2a): sancionar con una advertencia.
El apartado 89.25 con el apartado 58.2b): sancionar con apercibimiento.
El apartado 89.7 con el apartado 58.2h): ordenar que no se emita una certificación.
El apartado 89.25 con el apartado 58.2i): imponer una multa administrativa.
El apartado 89.3 con el apartado 58.3b): emitir dictámenes.
El apartado 89.5 con el apartado 58.3d): aprobar proyectos de códigos de conducta.
El apartado 89.9 con el apartado 58.3g): adoptar las cláusulas tipo de protección.

Diferencias:
En Ecuador en el año 2010, mediante la promulgación de la Ley del Sistema Nacional de Registro de Datos Públicos se creó el Sistema y la Dirección Nacional de Registro de Datos Públicos (DINARDAP), conformado por los registros: Civil, de la Propiedad, Mercantil, Societario, Datos de conectividad electrónica, Vehicular, de Naves y aeronaves, Patentes, de Propiedad intelectual y todos los registros de datos de las instituciones públicas y privadas que mantuvieren y administren por disposición legal información registral de carácter público. Respecto a la citada Dirección, el apartado 89.29 del proyecto de ley establece de forma específica que la Autoridad de Protección de datos controlaría el ejercicio del derecho de protección de datos en el tratamiento del responsable denominado DINARDAP. Según Luis Enríquez, es preciso excluir a la DINADARP la facultad de decidir qué datos son considerados como datos públicos, porque este organismo no podría ser imparcial para decidir la diferencia entre datos personales y datos públicos [21].

De acuerdo al proyecto de ley, en el Registro Nacional de Protección de Datos Personales no se incluiría un registro de las infracciones que es considerado en el

RGPD literal (u) apartado 57.1 y que contiene toda la información sobre la aplicación de los poderes correctivos de la Autoridad de Control.

En el apartado 89.20 del Proyecto de Ley se establece como función de la Autoridad llevar el registro de vulnerabilidades, esto se considera un error de competencia, pues la Autoridad de Control, no debe ser el organismo técnico sobre incidentes de seguridad porque no constituye un CERT o un CIRT, entidades que administran los registros de vulnerabilidades técnicas con base en los incidentes que afectan la seguridad de la información (que pueden o no afectar a la seguridad de datos personales). En su defecto, cuando el caso amerite, la Autoridad de Control podría en función de sus atribuciones solicitar la información técnica a los organismos que gestionan dichos incidentes.

En la redacción del Proyecto de Ley se redactan varias funciones relacionadas con la coordinación internacional, en un aspecto de forma se podría agrupar éstas en un menor número de atribuciones.

El Proyecto de Ley omite ciertos poderes de autorización y consultivos indicados en el RGPD, como son:
f) expedir certificaciones y aprobar criterios de certificación;
g) adoptar las cláusulas tipo de protección de datos;
h) autorizar las cláusulas contractuales;
i) autorizar los acuerdos administrativos; y
j) aprobar normas corporativas vinculantes.

Propuesta Nro. 47. Modificar Artículo 92. Funciones, atribuciones y facultades.
Corresponden a la Superintendencia de Protección de Datos las siguientes funciones, atribuciones y facultades:
(…)
Agregar:
- Realizar un seguimiento de cambios en el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales, en la medida en que tengan incidencia en la protección de datos personales;
- Llevar a cabo investigaciones sobre la aplicación de la presente Ley, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;
- Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos;
- Llevar a cabo una revisión de las certificaciones expedidas;
- Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del titular;
- Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones de la presente Ley, cuando proceda, de una determinada manera y dentro de un plazo especificado;
- Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento, y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales; y,
- Poner en conocimiento de las autoridades judiciales las infracciones de la presente Ley y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en la misma.

Modificar:
9. Dictar las cláusulas estándar de protección de datos, autorizar las cláusulas contractuales y los acuerdos administrativos; *y, aprobar las normas corporativas vinculantes;*

Reemplazar
Donde dice:
20. Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;
Reemplazar por:
20. *Llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con la facultad sancionadora;*

Artículo 59. Informe de actividad
Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

En el Proyecto de Ley no aplica en el ámbito de aplicación territorial

En el capítulo VII del RGPD, se hace mención al ámbito de aplicación territorial de la Unión Europea y al sentido de cooperación entre varias Autoridades de Control en Estados miembros. Por esta razón no se requiere articulados similares en el Proyecto de Ley:

CAPÍTULO VII Cooperación y coherencia
Sección 1. Cooperación y coherencia
Artículo 60. Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas
Artículo 61. Asistencia mutua
Artículo 62. Operaciones conjuntas de las autoridades de control
Sección 2. Coherencia
Artículo 63. Mecanismo de coherencia
Artículo 64. Dictamen del Comité
Artículo 65. Resolución de conflictos por el Comité
Artículo 66. Procedimiento de urgencia
Artículo 67. Intercambio de información
Sección 3. Comité europeo de protección de datos
Artículo 68. Comité Europeo de Protección de Datos
Artículo 69. Independencia
Artículo 70. Funciones del Comité
Artículo 71. Informes
Artículo 72. Procedimiento
Artículo 73. Presidencia
Artículo 74. Funciones del presidente
Artículo 75. Secretaría
Artículo 76. Confidencialidad

10. Recursos, responsabilidad y sanciones

10.1. Derecho a Reclamaciones

Artículo 77. Derecho a presentar una reclamación ante una autoridad de control
1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.
2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. Derecho a la tutela judicial efectiva contra una autoridad de control
1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.
2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.
3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.
4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento
1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.
2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. Representación de los interesados
1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y

ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.
2.Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. Suspensión de los procedimientos
1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.
2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.
3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

10.2. Derecho a indemnización

Artículo 82. Derecho a indemnización y responsabilidad
1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.
3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.
4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.
5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o

encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.
6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 73. Queja directa del titular del dato personal al responsable del tratamiento de datos personales: El titular de los datos personales podrá, en cualquier momento, de forma gratuita y por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar quejas sobre el contenido de los derechos, principios y obligaciones para hacer efectivas de forma directa sus peticiones, en especial aquellas relacionadas al acceso, rectificación o actualización, eliminación, oposición, limitaciones al tratamiento, portabilidad, notificaciones sobre violaciones a la seguridad, transferencia internacional a terceros países, entre otros.
Presentada la queja ante el responsable, este contará con un término de Cinco (5) días para contestar y notificar en debida forma sobre su respuesta afirmativa o negativa, y ejecutar lo que se le haya solicitado.

Artículo 74. Del inicio del procedimiento administrativo: La Autoridad de Protección de Datos Personales podrá iniciar de oficio o a petición del titular actuaciones previas, con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

Artículo 75. Reclamo administrativo ante la Autoridad de Protección de Datos Personales: En el caso de que el responsable del tratamiento no conteste a la queja en el término establecido en la presente ley, o, ésta fuere negativa, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se estará conforme al procedimiento establecido en el Código Orgánico Administrativo, la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales
Sin perjuicio de lo antes expuesto, el titular podrá presentar acciones civiles, penales y constitucionales a las que se crea asistido.

En los artículos 77, 78, 79, 80 y 81 del RGPD se establece de forma separada los derechos de los interesados acerca de: una tutela judicial efectiva en contra de la autoridad de control, un responsable o un encargado del tratamiento; y el derecho de ser representado por una organización. En los artículos 73, 74 y 75 del Proyecto de Ley únicamente se menciona los derechos del titular de presentar, en primera instancia, reclamos ante el responsable, y en segunda instancia presentar reclamos ante la Autoridad de control, sin hacer alusión a las posteriores acciones judiciales posteriores ni a su derecho de ser representado. En este aspecto, existe el criterio de que la legislación no debiera crear una acción especial para tutelar estos bienes jurídicos y simplemente debiera remitirse a las normas generales, o en todo caso señalar que va a ser procedente el recurso de protección [20].

Por otra parte la suspensión de procedimientos está relacionado con las acciones entre varios Estados miembros de la Unión Europea, que no aplica al ámbito nacional del proyecto de Ley analizado; esto es reemplazado en el proyecto de ley con el último

párrafo del artículo 75 en el que se indica que el titular podrá presentar acciones civiles, penales y constitucionales a las que se crea asistido.

En el artículo 82 del RGPD se detalla las consideraciones respecto a la indemnización por daños y perjuicios al que tiene derecho el interesado. Es el derecho que tienen los afectados a que se reconozcan acciones que directamente puedan interponer ante algún órgano jurisdiccional que les permita el pronto restablecimiento de su privacidad, intimidad o imagen afectada y la compensación por esos perjuicios o daños que deban soportar a consecuencia de toda intromisión ilegítima [20].

En este aspecto el apartado 2 de dicho artículo establece que un encargado únicamente deberá asumir la responsabilidad cuando no haya cumplido con las obligaciones del Reglamento dirigidas específicamente a los encargados o cuando haya actuado en contra de las instrucciones del responsable. En el apartado 82.1 no se establece la responsabilidad personal del delegado de protección de datos por el incumplimiento de la normativa en materia de protección de datos [5].

Propuesta Nro. 48. Añadir al final Artículo 75. Reclamo administrativo ante la Autoridad de Protección de Datos Personales.
(…)
Cualquier titular que haya sufrido un perjuicio, material o inmaterial, como consecuencia de una operación de tratamiento que no se atenga a presente Ley, tiene la potestad de presentar una reclamación ante la Autoridad de Control correspondiente, y en su caso, puede requerir una indemnización si se demuestra que sus derechos se han visto vulnerados.

10.3. Infracciones y Sanciones

10.3.1. Condiciones generales

Artículo 83. Condiciones generales para la imposición de multas administrativas
1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.
2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente **en cuenta**:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.
3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.
4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) las obligaciones del **responsable y del encargado** a tenor de los artículos 8, 11, 25 a 39, 42 y 43;
b) las obligaciones de los **organismos de certificación** a tenor de los artículos 42 y 43;
c) las obligaciones de la **autoridad de control** a tenor del artículo 41, apartado 4.
5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 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:
a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;
b) los derechos de los interesados a tenor de los artículos 12 a 22;
c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;
d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;
e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.
6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 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.
7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se

puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.
8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.
9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. Sanciones
1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.
2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

Medidas correctivas, infracciones y régimen sancionatorio
Artículo 76. Objeto y ámbito de aplicación: Los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, están sujetos a medidas correctivas, infracciones y al régimen sancionatorio establecido en el presente Capítulo.
En el caso de entidades pertenecientes al sector público, las resoluciones que determinen medidas correctivas o aplicación de régimen sancionatorio deberán ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos personales con la finalidad de que se inicien los procedimientos disciplinarios en contra de los servidores o funcionarios, por cuya acción u omisión se hubiese incurrido en alguna de las infracciones establecidas en la presente ley, sin perjuicio de la responsabilidad civil, administrativa y/o penal a la que hubiere lugar.

A diferencia del detalle establecido en el RGPD, en el Proyecto de Ley se puede encontrar las siguientes novedades:
-No se menciona a las entidades de certificación como sujetos de infracciones en el caso de incumplir con una correcta evaluación de la certificación o retirada de la certificación.
-No se establece que la autoridad de control es sujeto de infracción.
-No se exime de responsabilidad al Delegado de protección de datos.

El proyecto determina como posibles infractores a los responsables, los encargados y terceros; sin embargo, en los artículos posteriores sólo se define el tipo de infracciones para responsables y encargados, y no para los terceros. Además se redacta un párrafo específico para las infracciones de las organizaciones pertenecientes al sector

público, determinando que la autoridad replique los procedimientos sancionatorios contra los servidores públicos.

Propuesta Nro. 49. Modificar Artículo 76. Ámbito de aplicación del régimen sancionatorio.

Los responsables, encargados del tratamiento de datos personales *y organismos de certificación*, están sujetos a medidas correctivas, infracciones y al régimen sancionatorio establecido en el presente capítulo.
No será de aplicación al delegado de protección de datos el régimen sancionador establecido en esta materia.
En el caso de organizaciones pertenecientes al sector público, las resoluciones que determinen medidas correctivas o aplicación de régimen sancionatorio deberán ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos personales, con la finalidad de que se inicien los procedimientos disciplinarios en contra de los servidores o funcionarios, por cuya acción u omisión se hubiese incurrido en alguna de las infracciones establecidas en la presente ley, sin perjuicio de la responsabilidad civil, administrativa y/o penal a la que hubiere lugar.

Artículo 77. Medidas correctivas. En caso de incumplimiento de las obligaciones previstas en la presente ley, su reglamento, directrices, lineamientos *y* regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; o, transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de reestablecer el derecho vulnerado y evitar que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.
Las medidas correctivas podrán consistir, entre otras, en:
l. El cese del tratamiento bajo determinadas condiciones o plazos; y,
2. La imposición de medidas técnicas, jurídicas, organizativas o administrativas tendientes a garantizar un tratamiento adecuado de datos personales.

10.3.2. Infracciones

El RGPD no contiene una clasificación de las infracciones, compete al ámbito de la ley dicha clasificación. En virtud, que el RGPD no efectúa una calificación de las conductas proscritas [5], en este punto del análisis no existen parámetros de comparación con el Reglamento y se toma como referencia a la LOPDGDD.

En este aspecto la LOPDGDD se adapta a los preceptos del Reglamento de la siguiente manera:

- en los artículos 72 y 73 define las infracciones graves o muy graves, tomando como referencia las condiciones generales establecidas respectivamente en los apartados 83.4 y 83.5 del RGPD; y,
- en el artículo 74 califica como leves aquellas infracciones de carácter meramente formal de los preceptos citados del Reglamento.

Artículo 78. Implementación: La Autoridad de Protección de Datos Personales, en el marco de esta ley, implementará para cada caso las medidas correctivas, previo informe de la unidad técnica competente, que permita corregir, revertir o eliminar las conductas

contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.
Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:
1. Para el caso de **infracciones leves** se aplicará a los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, únicamente medidas correctivas; en el caso de incumplimiento de dichas medidas correctivas o que éstas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones leves establecidas en la presente ley.
2. En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso, terceros, se encuentren incursos en el presunto cometimiento de una infracción leve y éstos consten dentro del Registro Único de Responsables y Encargados incumplidos; la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,
3. En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción grave, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida.

Por su parte, el artículo 78 del Proyecto de Ley establece la creación del Registro Único de Responsables y Encargados incumplidos, como un paso previo a ejecutar el régimen sancionador para infracciones leves. Este artículo permitiría a la Autoridad de control aplicar una sanción únicamente al caso de responsables y encargados incumplidos, es decir que anteriormente hayan cometido alguna infracción. A pesar de esto, posteriormente en el artículo 83.2.b), se determina que también debe realizarse un análisis de la reiteración de la infracción, esto supondría una doble revisión de la reincidencia en el cometimiento de una falta: el análisis del artículo 78 y luego el análisis de lo dispuesto en el apartado 83.2.b)

Otras observaciones de los artículos 77 y 78 del proyecto de ley son:
- No se menciona a los organismos de certificación y en su lugar se menciona a los terceros.
- No se presenta una consideración para los presupuestos generales requeridos a fin de aplicar el principio de proporcionalidad.

Por lo expuesto, es pertinente definir la calificación de las infracciones (leves, graves y muy graves) y la proporcionalidad para la imposición de multas. Respecto a la proporcionalidad puede definirse en función del grado de cumplimiento a las medidas correctivas dispuestas previamente a los infractores; y paralelamente considerar la calificación de la infracción cometida. La experiencia muestra que el camino disuasivo, de reparación civil, puede ser más efectivo que las sanciones que se pudiesen establecer [20].

Propuesta Nro. 50. Modificar Artículo 78. Condiciones para la imposición de multas (implementación):
La Autoridad de Protección de Datos Personales, en el marco de esta ley, previo informe de la unidad técnica competente, aplicará para cada caso las medidas correctivas citadas en el artículo anterior, que permitan corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:
1. En el caso de que los responsables, encargados del tratamiento de datos personales *y organismos de certificación*, se encuentren incursos en el presunto cometimiento de una *infracción leve; la Autoridad de Protección de Datos Personales aplicará en primera instancia medidas correctivas. Si las medidas correctivas fueren incumplidas, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones leves establecidas en la presente ley***.**
2. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una *infracción grave; la Autoridad de Protección de Datos Personales; aplicará en primera instancia medidas correctivas. Si las medidas correctivas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones graves, activando para el efecto el procedimiento administrativo sancionatorio* y haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,
3. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una *infracción muy grave, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio* haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida.

En todos los casos, las sanciones previstas *se aplicarán en función del principio de proporcionalidad para lo cual se deberá verificar los siguientes presupuestos:*
a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
b) Reiteración de la infracción; es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar,
c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
d) Reincidencia, es decir, cuando la Infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, la Autoridad de Protección de Datos Personales notificará de la Resolución con la cual se establezca la infracción cometida a la autoridad de protección de datos, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancie las acciones y/o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente Ley tendrán responsabilidad extracontractual, que puede ser de carácter administrativa, civil o penal.

Sección 1a
Del responsable
Artículo 79. Infracciones leves. Se consideran infracciones leves las siguientes:

1. No tramitar, tramitar fuera del plazo previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;
2. No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones de seguridad y protección de datos personales cuando no exista afectación a los derechos fundamentales y libertades individuales de los titulares;
3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;
4 No mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; y,
5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales

Artículo 80. Infracciones graves: Se consideran infracciones graves las siguientes:
1. No implementar requisitos, mecanismos o herramientas administrativas, técnicas, físicas, organizativas y jurídicas a fin de garantizar que el tratamiento de datos personales se realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Utilizar información o datos para fines distintos a los declarados;
3. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
4. Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
5. No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las particularidades del tratamiento y de las partes involucradas;
6. No realizar evaluaciones de impacto al tratamiento de datos;
7. No implementar medidas técnicas, organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de los datos personales que hayan sido identificadas;
8. No notificar a la Autoridad de Protección de Datos Personales y al titular, las vulneraciones a la seguridad y protección de datos personales cuando afecte los derechos fundamentales y libertades individuales de los titulares;
9. No implementar protección de datos desde el diseño y por defecto,
10. No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
11. Elegir al encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
12. No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
13. No designar al Delegado de Protección de Datos Personales;
14. No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del auditor acreditado por la Autoridad de Protección de Datos Personales, y,
15. El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por Infracción leve.

Sección 2a
Del encargado
Artículo 81. Infracciones leves: Se consideran infracciones leves las siguientes:
l. No asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales.
2. No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
3. No permitir o no contribuir a la realización de auditorías o Inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por éste o por la Autoridad de Protección de Datos Personales; y,
4. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales

Artículo 82. Infracciones graves: Se consideran infracciones graves las siguientes:
1. No tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional:
3. No suscribir contratos de confidencialidad y manejo adecuado de datos personajes con el personal a cargo del tratamiento de datos personales, o quién tenga conocimiento de los datos personales;
4. No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5. No Implementar medidas preventivas y correctivas en la seguridad de los datos personales a efecto de evitar vulneraciones,
6. No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales una vez haya culminado su encargo;
7. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
8. Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia, y,
9. El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por Infracción leve.

En el Proyecto de Ley para el caso de las infracciones leves se verifica lo siguiente:

- Se define cinco infracciones para el responsable, cuatro infracciones para el encargado y ninguna para los organismos de certificación. Estas nueve infracciones en número están muy por debajo del número de obligaciones o derechos desarrollados anteriormente en el proyecto.
- Apenas cinco de las nueve infracciones calificadas como leves coinciden plenamente con las consideraciones del artículo 83.4 del RGPD.

- Cuatro infracciones leves son comparables con infracciones graves conforme las consideraciones del apartado 83.5 del RGPD, esto es, porque se refieren a una vulneración de principios básicos o de derechos del interesado; e incluso con las consideraciones del apartado 83.6 relacionado con el incumplimiento de medidas correctivas dispuestas por la Autoridad de Control podrían calificarse como muy graves.

En el Proyecto de Ley para el caso de las infracciones graves se verifica lo siguiente:
- Existe un total de veinticuatro infracciones graves para el responsable y el encargado, número cercano al de posibles incumplimientos definidos en el proyecto de ley.
- Apenas nueve de las veinticuatro infracciones graves coinciden plenamente con las consideraciones del artículo 83.4 del RGPD.
- Quince de las veinticuatro infracciones graves se podrían considerar infracciones leves conforme las consideraciones del apartado 83.4 del RGPD, esto es, porque en su mayoría se refieren a las obligaciones del responsable y encargado y no están en perjuicio de: principios y derechos del interesado; las normas para las transferencias y del cumplimiento de disposiciones de la Autoridad de control.

La prescripción de infracciones y sanciones es el plazo que se establece para la caducidad de la acción para perseguir la infracción o la exigencia de la sanción una vez que es firme. Es un supuesto de extinción de la responsabilidad que hubiera sido exigible al infractor y que difiere tanto de la prescripción de las sanciones como de la caducidad del procedimiento [5].

A diferencia de la LOPDGDD, en el proyecto de ley no se establece plazos de prescripción de las infracciones, sin embargo el Código Orgánico Administrativo de Ecuador regula el ejercicio de la función administrativa y señala que estos plazos son: 1 año para infracciones leves, 3 años para infracciones graves, y 5 años para infracciones muy graves [16].

Con las consideraciones expuestas, y con la numeración de los artículos precedentes a continuación se presenta la propuesta para el proyecto de ley, en lo relacionado a la calificación de las infracciones en materia de protección de datos personales.

Propuesta Nro. 51. Unificar y modificar. Artículo 79. Infracciones Leves.

Califican como infracciones leves las que se consideran que tienen un carácter meramente formal de incumplimiento a las obligaciones establecidas para el responsable, el encargado y los organismos de certificación; de los principios del tratamiento; y los derechos del titular; y son las siguientes:
1. El incumplimiento del principio de transparencia de la información proporcionada al titular, sea que la información se haya obtenido directamente de él o no, según lo establecido por el artículo 23 de la presente Ley.
2. La exigencia del pago de un canon para facilitar al afectado la información exigida por el artículo 23.
3. No atender las solicitudes de ejercicio de los derechos establecidos para el titular en los artículos 23 a 36.
4. No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo infracciones graves de esta Ley.
5. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 42 de la presente Ley.

6. La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este conforme lo establecido por el artículo 72.2 de la presente Ley.
7. El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello para evitar la infracción y se hubiese advertido de ello al responsable o al encargado del tratamiento.
8. Disponer de un Registro de protección de datos personales que no incorpore toda la información exigida por el artículo 90 de la presente ley.
9. La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación o vulneración de seguridad de los datos personales de conformidad con lo previsto en el artículo 55 de la presente Ley.
10. El incumplimiento de la obligación de documentar cualquier violación o vulnerabilidad de seguridad, de conformidad con lo previsto en el artículo 55 de la presente Ley.
11. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 57 de la presente Ley, salvo que hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación en cuyo caso es una infracción grave.
12. No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible, conforme lo establece el artículo 58 de la presente Ley.
13. El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme lo establecido en el artículo 63 de la presente Ley.

Propuesta Nro. 52. Unificar y modificar Artículo 80. Infracciones Graves.

Califican como infracciones graves las que se consideran una vulneración sustancial de las obligaciones establecidas para el responsable, encargado y los organismos de certificación, y son las siguientes:
1. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme lo establecido en el artículo 36 de la presente Ley.
2. El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.
3. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, conforme lo establecido en el artículo 52 de la Presente Ley.
4. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos establecidos en el artículo 50 de la presente Ley.
5. El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo establecido en el artículo 50 de la presente Ley.
6. La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el artículo 71.12 de la presente Ley.

7. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 72.2 de la presente Ley.
8. La infracción por un encargado del tratamiento, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 72.13 de la presente Ley.
9. No disponer del registro de protección de datos personales establecido en el artículo 90 de la presente Ley.
10. No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de protección de datos, conforme el artículo 90 de la presente Ley.
11. No cooperar con la Autoridad de Control en el desempeño de sus funciones en los supuestos no previstos en el artículo 81 de la presente Ley.
12. El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones o vulneraciones de seguridad de las que tuviera conocimiento.
13. El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación o vulneración de seguridad de los datos personales de conformidad con lo previsto en el artículo 55 de la presente Ley.
14. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 57 de la presente Ley. si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.
15. El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.
16. El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo.
17. No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.
18. La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.
19. Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 62 de la presente Ley.
20. El desempeño de funciones los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 89.5 de la presente Ley.
21. El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en el artículo 62 de la presente Ley.

Propuesta Nro. 53. Agregar Artículo 81. Infracciones muy graves.

Califican como infracciones muy graves las que se consideran una vulneración sustancial a los principios del tratamiento, derechos del titular, transferencias internacionales y los incumplimientos a resoluciones de la Autoridad de Control; y, son las siguientes:
1. El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 8 de la presente Ley.
2. El tratamiento de datos personales sin que concurra alguna de las condiciones de legitimidad del tratamiento establecidas en el artículo 10 de la presente Ley. c) El incumplimiento de los requisitos exigidos por el artículo 14 de la presente Ley para la validez del consentimiento.

3. La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.
4. El tratamiento de datos personales de las categorías especiales de datos personales, sin que exista el consentimiento establecido en el artículo 39 de la presente Ley.
5. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 39 de la presente Ley.
6. La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en el artículo 23 de la presente Ley.
7. La vulneración del deber de confidencialidad establecido en el artículo 8 de la presente Ley.
8. El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en la presente Ley.
9. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 64 a 69 de la presente Ley.
10. El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 89 de la presente Ley.
11. No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.
12. La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.
13. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

Propuesta Nro. 54. Eliminar Artículo 82.

10.3.3. Sanciones

Artículo 83. Sanciones por infracciones leves: La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:
1. Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente Ley serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 3% y el 9% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos:
a) La intencionalidad, misma que se establecerá en función a la conducta del infractor:
b) Reiteración de la infracción; es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que

se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar,
c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
d) Reincidencia, es decir, cuando la Infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

Artículo 84. Sanciones por infracciones graves: La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción grave conforme a los presupuestos establecidos en el presente Capítulo:
1. Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionado con una multa de entre diez (10) a veinte (20) salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% Y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la Imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos:
a) La intencionalidad, misma que se establecerá en función a la conducta del infractor:
b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero; hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igualo mayor gravedad a la que se pretende aplicar;
c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.
En el caso de que el responsable, encargado del tratamiento de datos personales o un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, la Autoridad de Protección de Datos Personales notificará de la Resolución con la cual se establezca la infracción cometida a la autoridad de protección de datos, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancie las acciones y/o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

Artículo 85. Sanciones por infracciones graves: *Se repite todo el texto del artículo 84*

Los artículos del proyecto de ley 84 y 85 son exactamente iguales, se presume que es un error de forma, que debe ser corregido con la eliminación del artículo 85.

En el RGPD se establece que las sanciones serán efectivas, proporcionadas y disuasorias. Al respecto, el salario básico unificado del Ecuador se encuentra fijado hasta diciembre 2020 en USD $ 400. Por lo que una multa de 10 salarios básicos equivale a USD $ 4.000, y de 20 salarios básicos equivale a USD $ 8.000, multas que serían impuestas a los servidores del sector público. No se define claramente si dichos

montos se aplicarían a cada uno de los servidores que participaron en las acciones de acción u omisión o al conjunto de servidores como efecto de responsabilidad solidaria.

Los servidores públicos de nivel operativo que manejan los datos personales son susceptibles de cometer infracciones cuando incumplen la normativa o el acuerdo laboral, el Proyecto de Ley plantea aplicar más sanciones pecuniarias al servidor público, adicional a la responsabilidad extracontractual de carácter civil, penal o administrativa. En este sentido se considera que la infracción respecto a la protección de datos personales se debe atribuir a la máxima autoridad del organismo público que se convertiría en el responsable del tratamiento, porque el servidor público no tiene esta condición, aunque sí deba responder en otras instancias por las infracciones cometidas.

En este aspecto la LOPDGDD, considera que las infracciones que fueren cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables son de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la infracción. La citada resolución debe ser notificada al responsable del fichero, así como al órgano del que dependa jerárquicamente. Asimismo, se establece la posibilidad de que el órgano sancionador proponga la iniciación de las correspondientes actuaciones disciplinarias, en el caso de que éstas procedan. Siendo el procedimiento y las sanciones a aplicar las establecidas en el régimen disciplinario de las Administraciones Públicas [18]. Como se detalla no se define multas económicas directas a los servidores públicos en aplicación de la Ley de Protección de datos.

En el proyecto de ley para las empresas privadas o públicas se establece un rango para la sanción económica en las sanciones leves y graves, respectivamente con rangos de entre: 3% al 9% y 10% al 17% del volumen de ingresos, sin embargo, estos rangos no establecen el porcentaje a utilizar, por ejemplo, cuándo utilizar el 3% o cuándo el 9% para las infracciones leves.

Respecto a los montos, como referencia, en la Ley Orgánica de Telecomunicaciones de Ecuador, las sanciones se establecen con rangos que van desde el 0,001% hasta el 0,1% del monto de referencia obtenido con base en los ingresos totales del infractor. Por esta razón, resalta que en el proyecto de ley de datos personales se determinen multas que pueden llegar al 17% sin que exista un sustento técnico-financiero que respalde dicho valor, más aún si el RGPD recomienda valores de hasta el 4%.

Propuesta Nro. 55. Modificar Artículo 83. Sanciones por Infracciones leves.
En el caso de que las medidas correctivas para infracciones leves fueren incumplidas por los infractores, la Autoridad de Protección de Datos Personales aplicará una multa de hasta el 1% sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Propuesta Nro. 56. Modificar Artículo 84. Sanciones por Infracciones graves.
En el caso de que las medidas correctivas para infracciones graves fueren por los infractores: cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales aplicará una multa de hasta el 2% sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Propuesta Nro. 57. Añadir Artículo 85. Sanciones por Infracciones muy graves.
La Autoridad de Protección de Datos Personales, aplicará una multa de hasta el 4% sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Artículos presentes en el Proyecto de Ley, no presentes en el RGPD:

Artículo 86. Volumen de Negocio: A efectos del Régimen Sancionatorio de la presente Ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del impuesto sobre el valor agregado y de otros impuestos directamente relacionados con la operación económica.

Artículo 87. Medidas provisionales o cautelares: La Autoridad de Protección de Datos Personales podrá aplicar medidas provisionales de protección o medidas cautelares contempladas en la norma procedimental administrativa.

Artículos presentes en el RGPD, no presentes en el Proyecto de Ley:

Disposiciones relativas a situaciones específicas de tratamiento
Artículo 85. Tratamiento y libertad de expresión y de información
1. Los Estados miembros **conciliarán** por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.
2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros **establecerán exenciones o excepciones** de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.
3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

En concordancia con lo establecido en el artículo 85 del RGPD, el Proyecto de Ley en el artículo 31 establece las excepciones específicas para conciliar el derecho a la libertad de expresión e información.

Artículo 86. Tratamiento y acceso del público a documentos oficiales
Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. Tratamiento del número nacional de identificación
Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizarán únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. Tratamiento en el ámbito laboral
1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.
2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.
3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas
1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.
2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

Para los cuatro artículos citados anteriormente y relacionados con el tratamiento de: documentos oficiales, número de identificación, ámbito laboral y datos de asociaciones religiosas, el Proyecto de Ley no hace ninguna mención en todo su cuerpo normativo.

Los capítulos X y XI del RGPD tienen relación con el Comité Europeo de Protección de Datos y las Directivas del Comité Europeo emitidas anteriormente a la expedición del RGPD, por tanto no tiene articulado análogo en el Proyecto de Ley.

CAPÍTULO X Actos delegados y actos de ejecución
Artículo 92. Ejercicio de la delegación
Artículo 93. Procedimiento de comité

CAPÍTULO XI Disposiciones finales
Artículo 94. Derogación de la Directiva 95/46/CE
Artículo 95. Relación con la Directiva 2002/58/CE
Artículo 96. Relación con acuerdos celebrados anteriormente
Artículo 97. Informes de la Comisión
Artículo 98. Revisión de otros actos jurídicos de la Unión en materia de protección de datos
Artículo 99. Entrada en vigor y aplicación

11. Disposiciones generales, transitorias, reformatorias y derogatorias del proyecto de ley

11.1. Disposiciones Generales

Primera*:* En lo dispuesto al procedimiento administrativo se estará a lo previsto en el Código Orgánico Administrativo
Segunda*:* En el ámbito del derecho de acceso a la información pública son aplicables las disposiciones de las leyes de la materia.
Tercera*:* En el ámbito de los datos personales registrables, son aplicables las disposiciones de las leyes de la materia.
Cuarta*:* La Autoridad de Protección de Datos Personales será responsable de coordinar las acciones necesarias con entidades del sector público y privado para el efectivo funcionamiento del Registro Nacional de Protección de Datos Personales.
Quinta*:* La Autoridad de Protección de Datos Personales será responsable de presentar informes bianuales de evaluación y revisión de la presente Ley, a la ciudadanía.
Sexta*:* Créase el Registro Único de Responsables y Encargados Incumplidos, en el cual se llevará un registro de los Responsables y Encargados del tratamiento de Datos Personales, que hayan incurrido en una de las infracciones establecidas en la presente Ley: mismo que tendrá fines sociales, estadísticos, preventivos y de capacitación, cuyo funcionamiento estará establecido en el Reglamento de la Ley de Protección de Datos Personales.
Séptima*:* El ejercicio de los derechos reconocidos en la presente norma podrá ser exigido por el titular independientemente de la entrada en vigor del régimen sancionatorio.

La Disposición General Sexta crearía el "Registro Único de Responsables y Encargados Incumplidos", aspecto que ha sido observado en el desarrollo del presente trabajo. Esto constituye un aspecto contradictorio al derecho de olvido digital que tendrían los titulares de datos personales, pero que no tendrían los responsables, encargados u organismo de certificación acerca de sus infracciones. Además no se define como se alcanzarían los fines sociales, estadísticos, preventivos y de capacitación, que se mencionan en el texto de la disposición. En virtud que las propuestas de cambios al Proyecto de Ley se han realizado en el sentido de eliminar el paso previo de consultar dicho Registro para aplicar el régimen sancionatorio, se propone también la eliminación de la citada Disposición.

Propuesta Nro. 58. Eliminar Disposición General Sexta

11.2. Disposiciones Transitorias

Primera: Las medidas correctivas y el régimen sancionatorio se aplicarán dentro de dos años contados a partir de la entrada en vigencia de la presente Ley, sin perjuicio de que en el transcurso de este tiempo los responsables y encargados del tratamiento se adecuen a los preceptos establecidos dentro de esta norma, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales.
Segunda: Todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial. El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.
Tercera: Los responsables y encargados del tratamiento de datos personales que hayan implementado los preceptos recogidos dentro de esta Ley antes del plazo señalado en la disposición Final Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales.
Cuarta: La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley será legítima, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada. El responsable de tratamiento deberá adecuar la transferencia internacional de datos personales a la presente norma en un plazo no mayor de dos años contados a partir de la publicación de la presente norma en el Registro Oficial
El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

La Disposición Transitoria Cuarta legitima cualquier transferencia internacional realizada antes de la vigencia de la Ley, lo que contempla un alto riesgo de que se ejecuten, de forma intencional, transferencias internacionales que no cumplan los principios universales de protección de datos personales, aprovechando el periodo del tiempo de adecuación que otorgue la nueva ley.

Propuesta Nro. 59. Modificar Disposición Transitoria Cuarta

La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley *deberá considerar la aplicación de todos los aspectos de seguridad de la información*, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada. *El responsable de tratamiento deberá adecuar la transferencia internacional de datos personales a la presente norma en un plazo no mayor de dos años contados a partir de la publicación de la presente norma en el Registro Oficial.*

11.3. Disposiciones Reformatorias

Primera: De la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Suplemento del Registro Oficial 557 del 17 de abril de 2002:
l. Suprímase las definiciones de intimidad, datos personales, datos personales autorizados del glosario de términos establecido en la Disposición General Novena.
2. Sustitúyase el texto del artículo 32 por el siguiente: "Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de

certificación de información garantizarán la protección de los datos personales conforme a los presupuestos establecidos en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales"

Segunda: Suprímase el inciso segundo del artículo 21 del Reglamento a la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos, publicado en el Registro Oficial 735 del 31 de diciembre de 2002.

Tercera: En la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del31 de marzo del 2010:
Sustitúyase:
a) El término Dirección Nacional de Registro de Datos Públicos por Dirección Nacional de Registros
Públicos;
b) El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;
c) El término Registro de Datos Púbicos por Registros Púbicos;
d) El término datos de carácter personal por datos personales;
e) El término dato público registral por la expresión datos públicos y datos personales registrables;
f) El artículo 6, por el siguiente:
"Art. 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, sólo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.
Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de Identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer.
La Directora o Director Nacional de Registros Púbicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.

2. Incorpórese:
a) En el artículo 31 referente a las atribuciones y facultades de la Dirección Nacional de Registros Públicos antes del numeral 14 el siguiente:
"14. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Púbicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto;
15. Tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos personales y su uso en todas las etapas del tratamiento, como por ejemplo, técnicas de disociación de datos, y,"
3. Suprímase del numeral 13 del artículo 31 lo siguiente: "y,".

4. Reenumerar el numeral 14 del artículo 31 por numeral"16".

Cuarta: En el Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016:
Sustitúyase:
1. El término Dirección Nacional de Registros de Datos Públicos por Dirección Nacional de Registros
Públicos;
2. El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros
Públicos;
3. El término Registro de Datos Públicos por Registros Públicos;
4. El término datos de carácter personal por datos personales; y
5. El término dato público registral por la expresión datos públicos y datos personales registrables.

Incorpórese:
En la Disposición General Séptima el siguiente inciso final. "La definición de términos relacionados con el derecho a la protección de datos personales estará conforme a lo establecido en la ley de la materia."

Quinta: En el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, publicado en el suplemento del Registro Oficial 899 del 09 de diciembre de 2016, sustitúyase la palabra confidencialidad por protección en el numeral 5 del artículo 67.

Sexta: En la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 el 18 de febrero de 2015:
1. Suprímase:
a) El inciso, segundo, tercer y cuarto del artículo 79;
b) En el primer inciso del artículo 83 lo siguiente: "(…) y seguridad de datos personales (…); y,
e) En el inciso primero del artículo 85 lo siguiente: "(…) como de seguridad de datos personales (…)"

2. Sustitúyase:
a) El artículo 78 por el siguiente:
Art. 78. Seguridad de los Datos Personales: Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

b) El artículo 81 por el siguiente:
Art. 81. Guías telefónicas o de abonados en general: Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados. Deberán ser informados, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales, de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías

c) El artículo 82 por el siguiente:

Art. 82. Uso comercial de datos personales: Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento conforme lo establecido en la Ley Orgánica de Protección de Datos Personales. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico.
Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personales de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados.

d) El artículo 83 por el siguiente.
Art. 83. Control técnico: Cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la seguridad e integridad de las redes, la Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.
Cuando, como consecuencia de los controles técnicos efectuados, quede constancia de los contenidos, se deberá coordinar con la Autoridad de Protección de Datos Personales para que:
a) Los soportes en los que éstos aparezcan no sean ni almacenados ni divulgados; y,
b) Los soportes sean inmediatamente destruidos y desechados
Si se evidencia un tratamiento ilegítimo o ilícito de datos personales, se aplicará lo dispuesto en la Ley Orgánica de Protección de Datos Personales.

Séptima: En el Reglamento a la Ley Orgánica de Telecomunicaciones, publicado en el suplemento del Registro Oficial 676 del 25 de enero de 2016 sustitúyase:
El artículo 120, por el siguiente:
Art 120. Protección de datos personales: Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, como por ejemplo, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la Ley Orgánica de Protección de Datos Personales, su Reglamento y las resoluciones emitidas por la Autoridad de Protección de Datos Personales, para el efecto la violación de esta garantía dará lugar a la Imposición de las sanciones previstas en el ordenamiento jurídico

2. El artículo 121, por el siguiente:
Art 121. Uso comercial: Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora;

salvo consentimiento del usuario, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.
Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento, conforme lo establece la Ley Orgánica de Protección de Datos Personales, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. Dicho instrumento debe contener lo determinado en la Ley Orgánica de Protección de Datos Personales, su Reglamento o las resoluciones que su Autoridad de Protección de Datos Personales dicte para el efecto. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías.
La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de las redes.

Octava: Sustitúyase del Capítulo III, del Título XIII, del Libro l. de la Resolución No. SB-2017-810, de 31 de Octubre 2017, que Codifica las Normas de la Superintendencia de Bancos:
El artículo 14, literal b por el siguiente: Las entidades financieras al tratar datos personales deberán apegarse a lo previsto en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y la normativa especializada emanada por la Autoridad de Protección de Datos Personales que dicte para el efecto.

11.4. Disposiciones Derogatorias

Primera: Deróguese el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial 557 del 17 de abril de 2002.

Segunda: Deróguese los articulas 80 y 84 de la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015.

Tercera: Deróguese el artículo 5 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del 31 de marzo del 2010.

Cuarta: Deróguense los artículos 11 y 12 y los numerales 2, 3, 4, 5, 8, 10, 11, y 12 de la Disposición General Séptima del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016.

Quinta: Quedan así mismo derogadas todas aquellas disposiciones de igual o menor jerarquía que se contrapongan con la presente Ley Orgánica.

12. Conclusiones

12.1. Conclusiones del trabajo

Producto del análisis comparativo entre el RGPD y el Proyecto de Ley de Protección de Datos Personales de Ecuador se ha encontrado los siguientes resultados.

a) Un hallazgo positivo, son las semejanzas encontradas en la definición de los principios y derechos porque representan en gran porcentaje el espíritu de la defensa del derecho humano de la protección de datos personales y expresan de manera coherente las generalidades más importantes del objetivo de la ley. Otras semejanzas se refieren a los aspectos estructurales entre los dos cuerpos normativos, como se describen a continuación:

1. La estructura básica de la norma, esto es: disposiciones generales, principios, derechos, medidas de seguridad, figuras de los involucrados y régimen sancionatorio.
2. Condiciones aplicables al consentimiento de menores de edad.
3. Principios en sus generalidades.
4. Derecho a la lealtad, transparencia e información.
5. Derecho de rectificación.
6. Posición del delegado de protección de datos.
7. Principio general de las transferencias.
8. Transferencias basadas en adecuación.
9. Transferencias basadas en normas corporativas.

b) En lo relacionado a las diferencias formales destaca el enfoque que necesita el derecho a la supresión u olvido digital, porque la redacción del artículo correspondiente debe considerar aspectos que salen del ámbito de la protección de datos personales, por ejemplo la libertad de acceso a la información y expresión, y la existencia de tecnologías como el “blockchain” que se basa en la no eliminación de los datos; y por ende existe una delgada línea entre el derecho al olvido digital y la no afectación a los citados aspectos. Seguidamente se enumeran otras diferencias formales encontradas, que pueden tener su explicación en la premura y el contexto político en el cual se entregó el proyecto de ley. Por lo expuesto, es recomendable recoger nuevos aportes, como el que se ofrece en presente trabajo, y otros de los diferentes actores involucrados para realizar un análisis pormenorizado que pretenda obtener artículos afinados, con el detalle suficiente que facilite la aplicación concreta y que, eliminando las ambigüedades deslizadas, permita lograr en el corto plazo los resultados buscados y los beneficios esperados:

1. Objeto de la ley, en cuanto a la protección específica de personas físicas y que además incluye garantizar los derechos digitales.
2. Finalidad, artículo presente que no tiene relación directa con la protección de datos personales.
3. Ámbito de aplicación material, en relación al soporte de los datos y al tipo de tratamiento.
4. Ámbito de aplicación territorial, debido a la ubicación del territorio ecuatoriano y la no pertenencia a la Unión Europea.
5. Definición de dato personal, en cuanto a la redacción de cualquier información que identifique a una persona.

6. Definición de tratamiento, debido a la amplitud del término “cualquier uso” de datos personales.
7. Definición de “seudonimización”, respecto a su inexistencia en la sección de definiciones.
8. Definiciones de transferencia y transmisión, en relación a que se definen como un único término, cuando la trasferencia debe referirse a un destinatario internacional y la transmisión a un encargado.
9. Falta de otras definiciones que tienen relación directa con el ámbito de aplicación territorial del RGPD.
10. Normas aplicables al ejercicio de derechos, artículo presente que define como actores a los “jueces competentes”.
11. Principios nuevos incluidos: consentimiento, que no necesariamente es un principio; y la aplicación favorable al titular.
12. Principio de Licitud, respecto a la prevalencia de los derechos fundamentales del interesado.
13. Principio de Licitud, sobre los fines para el tratamiento ulterior.
14. Consentimiento, en relación a la prestación de un servicio.
15. Calidad de los datos, respecto a quién debe definir la actualización los mismos.
16. Normativa especializada, porque no establece la prevalencia de los principios de la ley.
17. Derecho a ser informado, sobre intereses legítimos de terceros y de los destinatarios internacionales.
18. Derecho de acceso, con respecto a sus características, a la posibilidad de negarse a actuar y de cobrar un canon por peticiones repetitivas.
19. Derecho de supresión (derecho al olvido), en relación con la oferta de servicios dirigidos a menores, y a la petición realizada a un juez competente.
20. Derecho a la limitación del tratamiento, por la similitud con la definición del derecho de supresión y porque no especifica las condiciones para su ejercicio.
21. Derecho a la portabilidad, debido a las condiciones simultáneas que deben cumplirse para el ejercicio del derecho.
22. Derecho de oposición, respecto a que no define las condiciones necesarias.
23. Decisiones individuales automatizadas, porque no se excluye cuando se trata de las categorías especiales de datos.
24. Limitaciones, relacionado al caso específico de los derechos de eliminación, oposición y anulación, cuando se opongan al derecho a la libertad de expresión y opinión.
25. Excepción por normativa especializada, en cuanto a los principios que deben aplicarse.
26. Obligaciones del responsable, respecto a la adhesión a códigos de protección y llevar el Registro Nacional de Protección de Datos Personales.
27. Protección de datos desde el diseño, porque son igualmente responsables el responsable y el encargado.
28. Registro de las actividades de tratamiento, respecto a las condiciones a considerar para una pequeña o mediana empresa en el Ecuador.
29. Seguridad del tratamiento, respecto a la obligación simultánea para el responsable y el encargado.
30. Notificación de vulneración de seguridad, en relación a realizar un análisis del impacto sobre los derechos de los interesados.

31. Comunicación de una violación de la seguridad al interesado, en cuanto a que la Autoridad de control disponga realizar la notificación.
32. Evaluación de impacto, referida a qué condiciones la convierte en una obligación para el responsable.
33. Medidas de seguridad en el ámbito del sector público, artículo que no relaciona la existencia del Esquema Gubernamental de Seguridad de la Información del Ecuador.
34. Acceso a datos para atención a incidentes informáticos, en el que se establece las organizaciones permitidas.
35. Designación del delegado de protección de datos, respecto a la comunicación de la designación a la Autoridad de control.
36. Certificación, en relación a la autorización del funcionamiento de las entidades certificadoras.
37. Organismo de certificación, en relación a la acreditación de las entidades certificadoras.
38. Transferencias mediante garantías adecuadas, respecto a los casos en que se requiere previa autorización de la Autoridad de control.
39. Transferencias con excepciones para situaciones específicas, porque se contemplan casos adicionales como las transferencias bancarias y bursátiles
40. Funciones y poderes de la Autoridad de control, en cuanto a que no se establece ciertas facultades administrativas para autorizar: certificaciones, cláusulas tipo, acuerdos y normas vinculantes
41. Funciones y poderes de la Autoridad de control, en el registro estadístico de las vulneraciones de seguridad.
42. Derecho a indemnización, porque no se redacta de forma expresa.

c) Finalmente se listan las diferencias que, a criterio del autor de éste trabajo, representan distorsiones fundamentales del Proyecto de Ley con respecto al RGPD, y que además, generarían problemas importantes en la adecuada aplicación de la ley por las razones que se exponen en cada ítem:

1. Ámbito de aplicación material, en relación a la no aplicación de la ley para el tratamiento de datos de comerciantes, socios de personas jurídicas y servidores públicos. Significa una exclusión expresa de la defensa de los derechos de dichos grupos de personas físicas basada en el hecho de su actividad profesional y/o económica; esto se contrapone al principio constitucional de igualdad y no discriminación al que tienen derecho todos los ecuatorianos.
2. Consentimiento general, en relación a que no es requerido de forma explícita cuando se trata de transferencias a otros países. La diferencia se considera sustancial porque si los datos personales salen del límite nacional, se complica el ejercicio de los derechos del interesado como son: acceso, supresión, rectificación y eliminación; esto además dificulta el objetivo de disponer de un carácter internacional y coordinado con condiciones homogéneas en las regulaciones a nivel mundial.
3. Consentimiento relativo a categorías especiales de datos, en cuanto a que no se encuentra prohibido por defecto para el tratamiento de dichos datos. Este punto, aunque sutil, puede ser un aspecto que proporcione o no una gestión diligente en la aplicación de la ley, puesto que si el tratamiento de categorías

especiales de datos se encuentra prohibido por defecto, le permite a la persona física ser protegida también por defecto aun en el desconocimiento de la existencia de la ley, algo que toma mayor importancia en países en los cuales no se encuentra avanzada la cultura y la conciencia del derecho de protección de sus propios datos personales.

4. Tratamiento de datos relativos a condenas e infracciones penales, porque no se encuentra definido. La idea no es interferir en el derecho penal de los países, pero no se debe olvidar que el delincuente no ha perdido todos los derechos humanos fundamentales, y es por esto, que debe definirse la forma del tratamiento de sus datos en lo relacionado a la minimización, limitación de la finalidad y confidencialidad, cuando los casos así lo permitan.
5. Obligaciones del encargado, porque compartiría la responsabilidad con el responsable del tratamiento, es decir, el encargado sería corresponsable por naturaleza. Esto constituye una incongruencia porque la responsabilidad debe aplicarse al encargado únicamente cuando ha determinado por su cuenta las finalidades o ha incumplido las instrucciones del responsable, caso contrario no sería necesario la definición de las dos figuras y sólo se hablaría de responsables de primer y segundo nivel.
6. Funciones del Delegado de protección de datos personales, en relación a su posible responsabilidad administrativa, civil y penal. Esta redacción del proyecto de ley dista profundamente de la exclusión tácita con la que el RGPD ampara al Delegado porque considera que no puede en ningún caso asumir poder de decisión sobre los fines y los medios del tratamiento de datos.
7. Autoridad de control, en lo relacionado a su cuestionable independencia al formar parte del poder Ejecutivo. No existe ninguna motivación basada en los principios o defensa de derechos que respalde la existencia de una Autoridad subordinada al Presidente, todo lo contrario, se contradice el precepto de la ley; y, si los fines políticos del gobierno de turno no son éticos, podrían ponerse en perjuicio del objeto de la ley.
8. Ámbito de aplicación del régimen sancionatorio, porque no considera a los organismos de certificación. El posible accionar sin control para estos actores podría producir la creación de entidades que no cumplan estándares mínimos para la entrega de certificados en materia de protección de datos, creándose un peligroso mercado de compra y venta de sellos que enmascaren cualquier incumplimiento de los responsables, quienes incluso, con desconocimiento del tipo de certificado obtenido, asuman que su gestión es adecuada con base en la falsa confianza adquirida.
9. Condiciones para la imposición de multas y a las sanciones pecuniarias directas para los servidores públicos que no tienen la figura de responsables del tratamiento. Además de los aspectos concluidos en la falta de trato igualitario para los servidores públicos, las sanciones directas generan una sensación tal que todas las filtraciones de datos personales del sector público tienen como responsables principales a los servidores de nivel jerárquico inferior, y que las autoridades de los organismos públicos únicamente constituyen otras víctimas de la afectación. Esta inequidad de la responsabilidad ulterior no se compadece con el grado de preparación que deben tener las autoridades públicas, cuando asumen la responsabilidad de la

dirección estratégica de la organización, lo que también incluye el ámbito de la seguridad de los datos personales tratados.

10. Infracciones leves, porque no se consideran todas las obligaciones del proyecto de ley, ni las consideraciones generales del RGPD. Sorpresivamente el Proyecto de Ley establece apenas nueve infracciones leves, y algunas de ellas incluso podría calificarse como infracciones graves. Este hallazgo implica dos cuestiones; la primera que el articulado contiene obligaciones para las cuales un incumplimiento no tiene consecuencia, convirtiendo a parte de la ley en "letra muerta" porque carece de un efecto real; la segunda, una falta de estimación al impacto en la vulneración de principios básicos o de derechos que en cualquier caso deben ser calificadas como infracciones graves.
11. Infracciones graves, porque aunque se consideran la mayoría de las obligaciones del proyecto de ley, no se apegan a las consideraciones generales del Reglamento; esto es, son calificadas como graves a pesar de que no están en perjuicio de los principios y derechos del interesado; las normas para las transferencias y del cumplimiento de disposiciones de la Autoridad de control. Junto con la diferencia del ítem anterior, se genera en régimen sancionatorio ambiguo y con poca claridad para los administrados.
12. Infracciones muy graves, porque no se encuentran definidas. Con esta diferencia existe un alejamiento del marco normativo nacional que actualmente regula el ejercicio de la función administrativa del sector público, el Código Orgánico Administrativo, en el cual sí se definen las infracciones muy graves; en tal virtud, se complicaría la correspondencia de sanciones para los procedimientos administrativos de infracciones no definidas.
13. Sanciones, por el alto porcentaje del monto calculado con respecto al volumen de ingresos. La posibilidad de una sanción del 17% de los ingresos no guarda consideración con el principio de proporcionalidad y disuasión. Existe el riesgo que la estricta aplicación de la Ley signifique una encrucijada subjetiva para la Autoridad de control, en el momento que una sanción extremadamente alta pueda quebrar la estabilidad financiera del organismo sancionado, y esto represente la pérdida de servicios y de empleos; por esto, si es baja la probabilidad de la imposición de tales montos de sanción, se requiere cuestionar la definición de los montos observados.

Nivel estimado de concordancia entre el RGPD y el Proyecto de Ley

El proyecto de Ley contiene 90 artículos, número base con el cual se presenta la siguiente propuesta para una estimación porcentual de concordancia con el RGPD:

Numero de diferencias formales	42
Nivel de diferencia formal (42/90)	47%
Nivel de concordancia formal	53%

Numero de diferencias sustanciales	13
Nivel de diferencia sustancial (13/90)	14%
Nivel de concordancia sustancial	86%

Estimado nivel promedio de concordancia: 69.5%

12.2. Conclusiones sobre los objetivos planteados

Se ha logrado los objetivos inicialmente planteados, esto es, se ha conseguido: determinar un estado de la situación actual de la protección de datos personales en el Ecuador; una estimación de la medida en la que el proyecto de ley se alinea al RGPD; una determinación individual de cuáles y qué tipo (formales o sustanciales) son las diferencias en todos los artículos; y, la generación de 59 propuestas específicas de modificaciones a cada artículo del proyecto de ley, para que se adapte a los objetivos del RGPD.

12.3. Conclusiones sobre la planificación y la metodología

La planificación establecida en el génesis del presente trabajo ha sido ejecutada de forma estricta, aspecto que bajo el seguimiento permanente y guía oportuna del profesor consultor y la profesora responsable, ha permitido realizar los avances en los plazos esperados y entregar los productos conforme los requerimientos de la normativa académica.

La metodología utilizada en el desarrollo del trabajo ha sido la adecuada para realizar una comparación individual de la redacción del articulado bajo análisis. La extensión final de ésta memoria supera la cantidad de páginas sugeridas en los lineamientos de la Universidad, debido a que la metodología del trabajo requería una citación textual de todos los artículos de un Reglamento y un Proyecto de Ley.

13. Glosario

Los términos y acrónimos definidos a continuación excluyen a las definiciones citadas en los capítulos 2 y 3, porque dichas definiciones corresponden a conceptos en materia de protección de datos personales que, por la característica del presente trabajo, se han analizado de manera exclusiva en los citados capítulos.

Acceso	Facultad de cualquier interesado de exigir y obtener información de que dispone un responsable de tratamiento de sus datos personales.
Ámbito de aplicación	Sujeto obligado por lo establecido en la norma jurídica, u objetivo o fin perseguido por ella.
Automatizado	Dato que se encuentra informatizado, tratado a través de un ordenador.
Certificación	Actividad administrativa destinada a la evaluación de la conformidad con carácter voluntario con respecto a normas que les resulten de aplicación.
Código de conducta	Conjunto de reglas elaboradas por organizaciones con el objeto de mejorar las prácticas y elevar el nivel de protección de datos.
Confidencialidad	Condición de la información que no puede ser comunicada ni divulgada.
Dato	Información necesaria para el conocimiento de algo.
Delegado de protección de datos	Persona designada en asesorar en los casos legalmente previstos sobre las obligaciones en el cumplimiento de la normativa de protección de datos.

Derecho fundamental	Derecho de la persona que emanada de la dignidad humana, del libre desarrollo y de otros valores.
Destinatario de datos personales	Persona física o jurídica al que se transfieren datos personales, se trate o no de un tercero.
Encargado del tratamiento	Persona que trata los datos personales por cuenta del responsable del tratamiento.
Entidades de certificación	Entidad encargada de controlar el respeto de las normas de naturaleza voluntaria.
Evaluación del Impacto	Procedimiento que tiene por objeto identificar, describir y evaluar, los efectos directos e indirectos sobre la protección de datos personales.
Garantía adecuada	Aseguramiento de una obligación o de un nivel exigido en materia de protección de datos.
Indemnización	Compensación destinada a reparar al afectado por la privación de un derecho o un perjuicio provocado por un tercero.
Independencia	Situación en que se encuentra un sujeto que no está sometido a instrucción para la ejecución de decisiones.
Infracción	Conducta antijurídica tipificada en una ley como susceptible de ser sancionada.
Interesado	Persona física o jurídica que promueve el procedimiento por ser el titular de derechos o intereses legítimos.
Legitimidad	Cualidad referida al consentimiento de los ciudadanos.
Licitud	Conformidad a derecho.
Limitación	Restricción impuesta a un derecho o facultad.
Norma corporativa vinculante	Norma de las organizaciones que deben cumplir como una obligación interna.
Olvido digital	Derecho del interesado a que el responsable suprima todos sus datos personales.
Oposición	Facultad de impedir que los datos personales sean tratados, cuando existan motivos fundamentados y legítimos.
Portabilidad	Derecho del interesado que ha facilitados datos personales a transmitirlos en formato electrónico.
Principios	Axioma que plasma una determinada valoración de justicia constituida por doctrina que tiene aceptación.
Proyecto de Ley	Proyecto de Ley de Protección de Datos Personales de Ecuador.

Reclamación	Recurso, queja, solicitud, petición fundada en derecho.
Rectificación	Acción de reconducir algo a la exactitud que debe tener.
Registro	Órgano integrado en el que deben ser inscritos los datos necesarios para el ejercicio de una actividad.
Responsable del tratamiento	Persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento de datos personales.
RGPD	Reglamento General de Protección de Datos.
Riesgo	Ponderación de la probabilidad de un efecto perjudicial como consecuencia de un factor de peligro.
Sanción	Castigo impuesto al ciudadano por una administración por razón de la comisión de una infracción.
Seguridad de la información	Conjunto de actividades que se ocupan de proteger la información de amenazas que pudiera suponer pérdida o disminución de valor.
Superintendencia	Organismo técnico de vigilancia, auditoría, intervención y control de actividades o servicios públicos o privados.
Titular	Persona a la que están atribuidos determinados derechos.
Violación de seguridad	Cualquier efecto negativo que afecte o pudiera afectar a la seguridad de los datos personales.

14. Bibliografía

[1] Asamblea Nacional del Ecuador (2019). *"Proyecto de Ley de Protección de Datos* Personales*"*. Quito-Ecuador. [Consulta: 19 de octubre de 2020]. < *https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-proyecto-de-ley-organica-de-proteccion>*

[2] Parlamento Europeo y Consejo de La Unión Europea (2016). *"Reglamento General de Protección de Datos (RGPD)".* Bruselas. [Consulta: 19 de octubre de 2020]. <https://gdpr-info.eu/>

[3] Cañabate, Josep; et al. (2019). *"Legislación sobre protección de datos personales".* Barcelona: Universitat Oberta de Catalunya.

[4] Recio, Miguel (2019). *"Protección de Datos Personales en la Era Digital"*. Bogotá - Colombia: Pontificia Universidad Javeriana. [Consulta: 3 de noviembre de 2020]. <https://courses.edx.org/courses/course-v1:JaverianaX+GDD1.1x+1T2020/19ae190a7f44467c8dde4a1644829c95/>

[5] Palomar Alberto, Fuertes Javier (2019). *"Práctico Protección de datos de carácter personal"*. España. [Consulta: 20 de octubre de 2020]. <https://app-vlex-com.biblioteca-uoc.idm.oclc.org/#/sources/practico-proteccion-datos-personales-21717>

[6] Agencia Española de Protección de Datos (2018). Publicaciones de la Agencia Española de Protección de Datos. España. [Consulta: 20 de octubre de 2020]. <https://app-vlex-com.biblioteca-uoc.idm.oclc.org/#/search/jurisdiction:ES/publicaciones+agencia/sources/21826>

[7] Garriga Domínguez, Ana (2016). *"Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua"*. Madrid: Dykinson. [Consulta: 21 de octubre de 2020]. <https://app-vlex-com.biblioteca-uoc.idm.oclc.org/#/sources/nuevos-retos-proteccion-datos-personales-14328>

[8] Calder, Alan (2017). *"Reglamento General de Protección de Datos (RGPD) de la UE: Una guía de bolsillo"*. Renio Unido: O'Reilly Online Learning Platform Academic Edition. [Consulta: 21 de octubre de 2020]. <https://learning.oreilly.com/library/view/reglamento-general-de/9781849288859/?ar>

[9] Bojalil, Paulina; Vela-Treviño, Carlos, Baker McKenzie, (2019). Blog: *"Despuntan las reformas en materia de protección de datos en América Latina".* [Consulta: 28 de septiembre de 2020]. <https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina>.

[10] Sitio web de la Unión Europea (2020). Sección: "*Decisiones de Adecuación*" [Consulta: 28 de septiembre de 2020]. <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>

[11] VLex Ecuador (2020). Búsqueda específica: "*Ley protección de datos Ecuador*" [Consulta: 28 de septiembre de 2020]. <https://vlex.ec/tags/ley-proteccion-datos-ecuador-567599>

[12] Ministerio de Telecomunicaciones de Ecuador (2019), *"Guía para tratamiento de datos personales en la administración pública central"*. [Consulta: 21 de octubre de 2020]. < https://www.gobiernoelectronico.gob.ec >

[13] Servicio de Rentas Internas de Ecuador (2020). "*Régimen impositivo para microempresas*". [Consulta: 21 de octubre de 2020]. <https://www.sri.gob.ec/web/guest/regimen-impositivo-para-microempresas>

[14] Ministerio de Telecomunicaciones de Ecuador (2020). "*Esquema Gubernamental de Seguridad de la Información (EGSI)*" [Consulta: 21 de octubre de 2020]. <https://www.gobiernoelectronico.gob.ec/egsi-v2/>

[15] Consejo de Participación Ciudadana y Control Social (2016). "*Designación de Autoridades*." [Consulta: 19 de noviembre de 2020]. <http://www.cpccs.gob.ec/designacion-de-autoridades/superintendentes/>

[16] Registro Oficial Nro. 31 (2017). "*Código Orgánico Administrativo*". [Consulta: 19 de noviembre de 2020]. <https://www.gob.ec/regulaciones/codigo-organico-administrativo>

[17] Registro Oficial Nro. 439 (2015). "*Ley Orgánica de Telecomunicaciones*". [Consulta: 28 de septiembre de 2020]. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf>

[18] Pérez, Dolores (2017). *"Ley de Protección de datos"*. Segunda Edición. Málaga: Editorial ICB. [Consulta: 21 de octubre de 2020]. <https://elibro.net/es/lc/uoc/titulos/106146>

[19] Rebollo, Lucrecio; et al. (2016). *"El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente"*. Madrid: Dykinson. [Consulta: 22 de octubre de 2020]. <https://app-vlex-com.biblioteca-uoc.idm.oclc.org/#/sources/derecho-a-la-proteccion-de-datos-en-espa-a-y-argentina-origenes-y-regulacion-vigente-12281>

[20] Pfeffer, Emilio (2005). *"Comentarios a proyectos de ley relativos a la protección de datos personales en Chile"*. Chile: Red ALYC. [Consulta: 24 de octubre de 2020]. <https://www.redalyc.org/pdf/197/19730126.pdf>

[21] Enríquez, Luis (2017). *"Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales"*. Revista de Derecho No. 27. Quito-Ecuador: Universidad Andina Simón Bolívar - Corporación Editora Nacional. [Consulta: 24 de octubre de 2020]. < http://repositorionew.uasb.edu.ec/handle/10644/5945>

[22] Sacoto, Susy (2020). *"Derecho a la eliminación de datos personales atendiendo al principio de finalidad"*. Guayaquil - Ecuador: Universidad Católica Santiago de Guayaquil. [Consulta: 24 de octubre de 2020]. <http://192.188.52.94:8080/handle/3317/14533>

[23] Berrocal. Ana (2019). *"Estudio jurídico-crítico sobre la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*". Madrid: Editorial Reus. [Consulta: 23 de octubre de 2020]. <https://elibro.net/es/lc/uoc/titulos/128256>.