Universidad Militar Nueva Granada

Facultad de Derecho

TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES, ANÁLISIS COMPARATIVO ENTRE LEGISLACIÓN COLOMBIANA Y NORMATIVIDAD EUROPEA

Director: Dr. Juan Carlos Villalba Cuéllar

Trabajo De Grado presentado como requisito para optar al título de:

Abogado

Cindy Daniela Saboya López

German Ricardo Vargas Reyes

Colombia – Bogotá, 02 de septiembre de 2022

Contenido

CONTENIDO

INTRODUCCIÓN.

La protección de los datos personales cobró importancia los últimos decenios y el contexto de una economía social del mercado, sistema acogido por la Constitución Política de 1991 (Alarcón, 2018), favoreció la creación de un sistema legal de regulación de la materia. Hoy en día es necesario comprender la importancia que cobran los datos personales y el papel que juega su protección dentro de los sistemas sociales y jurídicos, como consecuencia del cambio de paradigma que se ha originado con la revolución 4.0 en donde la recopilación y procesamiento de los datos se dan con mayor facilidad; no solo a nivel local, sino internacional, cobrando especial preponderancia como lo menciona Botero (2016) quien afirma que "a información se ha convertido en uno de los activos más importantes nos solo en los negocios, sino en cada situación de la vida cotidiana en todos sus aspectos sociales, empresariales, académicos y de relacionamiento en el estado."(p. 1). Otros autores, como Caballero (2017) reafirman la postura anterior, mencionando que: "Gracias a las nuevas tecnologías y especialmente al comercio electrónico, la información y su tratamiento han experimentado en los últimos años un valor desconocido en los órdenes económicos, sociales y personales" (p.2).

El derecho a la protección de datos fue definido como "la facultad conferida a las personas para actuar *per se* y para exigir la actuación del Estado con el fin de obtener la tutela de los diversos derechos que pueden verse afectados en virtud de aquellas operaciones de tratamiento de los datos de carácter personal que les conciernen" (Pucinelli, 2004, p. 8). En el derecho colombiano su primer antecedente fue la protección del habeas data derivado de los postulados de la Constitución Política de 1991, que consagra el derecho a la información como derecho fundamental, posteriormente la Ley 1266 de 2009 que reguló aspectos del tratamiento de datos en el sector

financiero y posteriormente la Ley 1581 de 2012, que introdujo un marco de regulación más amplio y detallado en la materia, lo cual generó unos desarrollos importantes derivados de su puesta en práctica (López-Oliva, 2017). De tal manera el cumplimiento de la normatividad en datos personales hoy en día involucra protección de derechos e intereses que se relacionan con el derecho público y el derecho privado, dado que las empresas, de cualquier naturaleza, son los principales recolectores de datos. Al respecto señala Peña que el equilibrio entre el ejercicio de la innovación empresarial y la protección de datos es un eje importante necesario para el desarrollo de la sociedad de la información (2021). Además, el carácter de derecho fundamental, ligado directamente con el derecho a la intimidad, puede abrir paso a nuevas consideraciones y alcances de la protección de datos en la era de la globalización, perspectiva que según Savaris abre paso a nuevas consideraciones de alcances de derechos humanos como parte de los derechos intrínsecos de una persona al nacer (2012).

Así las cosas, en el ámbito colombiano la Ley 1581 de 2012, define dato personal como *"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*, persiguiendo como fin el pleno conocimiento de los ciudadanos de sus datos, el derecho a la rectificación y/o actualización, cuyo fundamento se encuentra respaldado en los principios de la transparencia y acceso a la información, según las limitaciones que establece la Ley.

Dentro del ámbito de los derechos y garantías constituciones, el derecho habeas data es aquel que según la reflexión hecha por Ruiz (2016), el cual consiste en un derecho que se otorga a "*los titulares de datos personales para controlar la información que sobre ellos este recolectada en las entidades administradoras de bases datos, para conocer, actualizar rectificar o excluir dicha información; así como también reservarse su consentimiento para divulgarla sin autorización*

previa" (p.13), siendo esta una definición mucho más amplia y acorde con diferentes pronunciamientos de la Corte Constitucional, en donde se ha dado un importante desarrollo jurisprudencial del principio de autodeterminación informática, tal como lo expreso esta corporación en la sentencia SU-082 de 1995 en donde se cuestionó:

> *¿Cuál es el núcleo esencial del habeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales" (Sentencia SU-082/95, 1995)*

En tal sentido y dadas las condiciones de avances tecnológicos en aumento durante la última década, y las necesidades de relacionamiento internacional por parte del Estado Colombiano, llevaron al entonces presidente Juan Manuel Santos, a buscar una alternativa legislativa que permitiera no solo el ejercicio al derecho de habeas data, que hasta la fecha era una derecho que se protegía por vía jurisprudencial o se limitaba a un solo sector, como es el financiero, sino también que estuviera en concordancia con la normativa internacional, quienes como parte de sus políticas de relación de negocios solicitaban una normatividad general y estable en la protección de datos.

Como resultado surge la Ley 1581 de 2012, la cual si bien es cierto fue un avance significativo para la época, hoy en día se queda corta respecto de nuevas dinámicas sociales, como, por ejemplo lo fue primero el auge de internet y la contratación por medios electrónicos (Villalba, 2008), Martínez (2018) "la nueva revolución industrial, la implementación de soluciones tecnológicas, la inteligencia artificial, el Blockchain, el Big Data, entre otros". (p.1). Lo anterior, va de la mano con un aumento considerable, como lo es, según Walters (2018) el análisis de datos es un campo

emergente en las últimas décadas y, más recientemente, un campo emergente en el sector legal. (p-10), lo que implica la recolección, análisis y tratamiento de gran cantidad de información.

Así las cosas, muchos de los datos circulan sin control sobre dichas herramientas, por lo que como lo establece Angarita (2012): "*existe un flujo transfronterizo de datos y las regulaciones sobre la materia deben buscar que los datos de los ciudadanos de un país, no disminuya cuando los mismos deben ser exportados o transferidos a otros países*" (p.12). Por lo anterior, y con el objetivo de realizar un ejercicio de derecho comparado, se busca identificar cuáles son los vacíos normativos de la legislación colombiana frente al tratamiento de datos personales, en contraste con el marco europeo en la Regulación general de Datos Personales, Reglamento 2016/679, el cual hoy en día es un referente a nivel mundial en este tema, con el objeto de buscar el fortalecimiento de la legislación nacional y la garantía real y material al derecho de habeas de data de la sociedad colombiana.

Para este fin esta monografía, dentro del marco metodológico de una investigación de tipo dogmático jurídico, buscará realizar un ejercicio de análisis normativo comparativo entre la legislación colombiana, tendiente a la regulación de protección y tratamiento de datos personales y el Reglamento 2016/679 de la Unión Europea. Se busca responder la siguiente pregunta problema ¿Cuáles son los posibles vacíos normativos en la legislación colombiana relativa al tratamiento y protección de datos personales en comparación con lo establecido por la Unión Europea? Partiendo de la hipótesis que la legislación colombiana tiene avances importantes, pero también rezagos normativos que deben corregir. Para tal fin se ha planteado como objetivo principal analizar comparativamente la legislación colombiana respecto del tratamiento y uso de datos personales con la regulación general para la protección de datos establecido por la Unión Europea con miras a identificar posibilidades de mejora para la norma nacional. Surgen entonces

como objetivos específicos el análisis de cada uno de los subtemas que estas normas abarcan para así determinar coincidencias y posibles falencias de la norma colombiana. En este sentido, primero se efectuará un análisis sobre las Ley 1581 de 2012, la cual es la generalidad, para luego entrar a validar los alcances existentes en materia de protección de datos por medio de las Resoluciones y/o Decretos expedidos por el Gobierno Nacional. Seguidamente, se analizará el marco común europeo, con el fin de encontrar diferencias y/o similitudes respecto de los conceptos de datos personales, qué tipo de información y/o datos son susceptibles de protección, los derechos de los titulares de los datos, las obligaciones de quienes hacen el tratamiento de los datos, los mecanismos de control a cargo de las autoridades. Se quiere llegar a plantear un comparativo general que permita identificar el estado actual normativo del derecho colombiano frente al régimen más moderno en la materia en derecho comparado con el objetivo ser necesario, plantear posibles cambios al régimen colombiano, con el ánimo de suplir eventuales vacíos normativos que se han generado por las nuevas dinámicas sociales y tecnológicas en la recolección de información, los cuales no se encuentran debidamente regulados por la Ley 1581 de 2012 y demás decretos reglamentarios expedidos por el Gobierno Nacional, lo que puede tener consecuencias para los titulares de los datos, quienes podrían ver vulnerado el derecho fundamental al habeas data, dispuesto constitucionalmente en nuestro ordenamiento jurídico.

Resulta en este sentido importante la presente investigación, como una propuesta de mejora a la norma que actualmente rige el tratamiento y protección de datos dentro del territorio colombiano, evitando de esta forma el no goce efectivo del derecho al habeas data, como una extensión de la personalidad de los titulares de la información, así como una oportunidad para que los responsables y/o encargados del tratamiento de los datos, cuenten con unas reglas y parámetros lo suficientemente claros en lo que respecta a las nuevas dinámicas sociales, que implican el uso de

las tecnologías de la información, Blockchain, Big data y *cloud computing* en la recolección, procesamiento, almacenamiento, flujo y eliminación de la data.

CAPÍTULO I. ANTECEDENTES REGULATORIOS

A continuación, se plasmarán los hitos más importantes para el desarrollo normativo, en lo que respecta al tratamiento y protección de datos personas, tanto en el ámbito colombiano, como dentro de la Unión Europea.

Caso Colombiano

Los avances en términos tecnológicos han sido de gran crecimiento en las últimas dos décadas, y paralelamente con este desarrollo, también han visto cambios estrepitosos en el mundo digital y la interacción que la sociedad tiene con el mismo. La digitalización en la prestación de los servicios y el aumento de usuarios en las redes sociales ha dejado expuesta la necesidad de otorgar los datos personales como una condición de acceso a los mismos. Esta situación no es ajena para los organismos internacionales y locales, quienes en la búsqueda de salvaguardar el uso adecuado de la información han desarrollado regulaciones que permiten conseguir dicho objetivo. Sin embargo, en la medida que la digitalización se incrementa y empieza a ser una herramienta eficaz para todo tipo de servicios, la regulación debe también avanzar para asegurar que los datos personales de quienes son beneficiarios de ellos sean protegidos y que exista una entidad supervisora que materialice esta protección. Acorde con lo anterior Monsalve (2015) afirma lo siguiente:

> El nuevo significado de la información y la utilización generalizada de las redes electrónicas impone notables exigencias de adaptación al ordenamiento jurídico, que van más allá de la simple actualización de sectores concretos, afectando al derecho en su conjunto, pues la inmaterialidad y la ubicuidad características de la información en el entorno digital condicionan ahora decisivamente tanto la posibilidad de establecer relaciones como

> la configuración de estas, así como la mayor importancia del comercio internacional de servicios y de los activos intangibles para las empresas (p. 19)

Así las cosas, en Colombia, desde la Constitución del 1991, se consagró la figura del HABEAS DATA, como aquel instrumento que le permite a cualquier persona conocer, actualizar y rectificar la información contenida en las bases de datos y en archivos de cualquier entidad, bien sea pública o privada. Según la Corte Constitucional este derecho fundamental "es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales" (Corte Constitucional, sentencia T729 de 2002). Por lo cual la carta política en su artículo 15 establece, que el tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Al respecto, la Corte Constitucional, manifestó en sentencia T-433 de 1994, con ponencia del magistrado Eduardo Cifuentes Muñoz, que el derecho al habeas data cumple una función de protección respecto de todas las personas contra el posible peligro o abuso de la información, de manera que garantice a todo individuo el derecho a la autodeterminación informativa (Sentencia T-443/94, 1994). Lo anterior va en línea con lo propuesto por Jiménez, W. G. & Meneses, O. (2017), quienes mencionan que, con la implementación de nuevas tecnologías, es necesario tener un mayor control sobre la protección de datos personales, por ejemplo, en ámbitos como las redes sociales. (p. 52)

Continuando con el desarrollo legislativo para el año 2010, el gobierno de Juan Manuel Santos, consciente que la automatización en los procesos de recolección y tratamiento de datos

personales era cada vez más común y que dicha actividad traía consigo la incertidumbre de conocer la finalidad y uso que se le otorgaba a estos datos, a través de sus ministros del Interior y de Justicia, de Comercio, Industria y Turismo y de Tecnologías de Información y las Comunicaciones, presentan el proyecto de ley estatutaria, por medio de cual se dictaban las disposiciones generales para la protección de datos personales.

El objetivo de este proyecto de ley fue que, en el proceso de recolección, almacenamiento, registro, uso o divulgación de los datos personales de los usuarios, se garantizara el otorgamiento del consentimiento por parte del titular, para que los datos fueran utilizados legítimamente por parte de un tercero con los fines que se le indicaban. Asimismo, la obligación de emplear altos estándares de calidad en el manejo de la información, al tiempo que se le otorgo una clara herramientas al titular para exigir medidas concretas de protección frente a cualquier vulneración de que pudiera ser víctima. (Gaceta del Congreso, 2010a)

Si bien, para el momento en que se presentó el proyecto de ley, existía y aún es vigente, la Ley 1266 de 2008, cuyo objeto asimismo es la protección del derecho de hábeas data, su aplicabilidad estaba limitada a las bases de datos que contenían información financiera, crediticia, comercial y de servicios provenientes de terceros países, por lo que, la protección al derecho fundamental no era integral. Así las cosas, finalmente fue la Corte Constitucional la que determinó el alcance y aplicabilidad de dicho derecho, y en diversas disposiciones determinó la necesidad de contar con una norma que garantizara el derecho de hábeas data de forma integral.[1]

[1] Solo por mencionar algunas sentencias hito, antes de la promulgación de la Ley 1581 de 2012, la Corte Constitucional de Colombia abordo el derecho al habeas data y el tratamiento de los datos personales en pronunciamientos como los analizados en sentencias C-993/04, C-981/05, T-648/12, SU458/12 y C-540/12.

Con el proyecto de ley estatutaria, que hoy en día es la Ley 1581 de 2012, se le otorgaba al titular de la información, una verdadera reclamación por vía administrativa que podía ser ejercida ante cualquier vulneración al derecho de hábeas data, acción de carácter subsidiario a la acción de tutela, medio principal utilizado entonces para garantizar la protección efectiva de este derecho.

Igualmente, el proyecto de ley presentado en 2010 buscaba que Colombia con la expedición de esta Ley, fuera considerado un país seguro para la protección de datos personales ante la comunidad europea, puesto que sus disposiciones incorporaban las mejores prácticas internacionales, dentro de ellas las establecidas por la directiva europea 95/46, antecedente de la actual Regulación General de la Protección de Datos de la misma organización.

En un principio, el proyecto de ley fue presentado con nueve títulos y 29 artículos, a saber:

- El título I Y II hacía referencia al objeto, ámbito de aplicación, definiciones y principios rectores de la Ley.
- El título III hace referencia los datos sensibles que afectan la intimidad del titular y cuyo uso indebido puede generar discriminación; y también hace referencia explícita a la protección especial de los datos de los niños, niñas y adolescentes.
- El título IV establece los derechos de los titulares de la información y determina las condiciones y requisitos cuyo cumplimiento es necesario para que el tratamiento de los datos personales sea jurídicamente viable. Dentro de las disposiciones más destacables está el consentimiento informado para el manejo de los datos personales.
- El título V, define el procedimiento para la atención de las consultas formuladas por los titulares o sus causahabientes a los responsables o encargados del tratamiento de datos.

- Seguidamente, el título VI, establece los deberes del responsable del tratamiento de datos y la capacidad que tiene esta persona de exigir el acatamiento de las condiciones de seguridad y privacidad.

- El título VII, hace referencia a la autoridad de control, ejercido por la Superintendencia de Industria y Comercio, describe las funciones como la entidad de control de habeas data y las sanciones que se pueden imponer por la vulneración del derecho, finalmente, establece la creación del Registro Nacional de Bases de Datos en el cual se deben inscribir quién realicen tratamiento de datos personales.

- El título VIII, establece el carácter prohibitivo de transferir datos personales de ciudadanos colombianos a terceros países. Y finalmente,

- El título IX, establece otras disposiciones en relación con la destinación de las multas prevista en la Ley 1266 de 2008. (Gaceta del Congreso, 2010a)

En el primer debate del proyecto de ley es importante mencionar, se hizo la modificación del artículo 2 numeral b, en cuanto se debe respetar los datos privados y que no pueden ser públicos a menos que exista autorización consentida del titular o presente algún tipo de peligro real y justificado a las seguridad y defensa nacional. En el artículo 4, se adicionó al numeral B y F, en cuanto a que el tratamiento no podría ser diferente a la finalidad autorizada por el titular o la Ley. A los artículos 17 y 18 se adicionaron deberes a los responsables del tratamiento y a los encargados del uso de los datos. En el artículo 19 se adicionó que el ente de control debe crear la Delegatura de Protección de Datos y en artículo 21 adicionó la función de requerir colaboración nacional y extranjera cuando se afecte el derecho de ciudadanos colombianos en el exterior. Se creó el artículo 29, el cual contempla como disposición especial el manejo que debe darse específicamente de no

publicar en el registro de antecedentes la información referente a penas cumplidas y prescritas. (Gaceta del Congreso, 2010b)

En segundo debate del proyecto de ley, se realizaron modificaciones al artículo 2, en cuanto a los datos que tengan fin de inteligencia y contrainteligencia y los límites y reservas que este tipo de datos puedan tener. En el artículo 5, de los datos sensibles se adicionan otras definiciones para aquellos que pertenecen a organizaciones que trabajan con derechos humanos, y al artículo 29 se adicionó el parágrafo 2 en el que se garantiza la disponibilidad de la información electrónica sobre el certificado de antecedentes judiciales, en la página de la entidad. Además, se adicionó el artículo 30 sobre los datos de inteligencia y contrainteligencia y el artículo 31 sobre el valor probatorio y la reserva de los informes de inteligencia y contrainteligencia. (Gaceta del Congreso, 2010c)

El informe de conciliación confirmó la adición del artículo 30 y 31 del segundo debate, los cuales fueron declarados inexequibles en la sentencia C- 748 de 2011, con ponencia del magistrado Jorge Ignacio Pretelt Chaljub, se declaró exequible la Ley en su articulado exceptuando los artículos 27 y 29 por vicios de fondo y los ya mencionados cuya inclusión no atendió el principio de consecutividad de los artículos 157 y 160 de la Constitución, por lo cual la Corte los declaró inexequibles.

Aunado a ello, el Ministerio de Comercio, Industria y Turismo mediante Decreto 1377 de 2013, posteriormente unificado por el Decreto 1074 de 2015, por medio del cual se reglamentó de forma parcial la Ley 1581 de 2012, estableció excepciones de las disposiciones contenidas en la citada Ley, como por ejemplo las bases de datos de carácter doméstico o personal, las cuales se realizan en el ámbito de la vida privada o familiar de las personas naturales. En adición se realizó la incorporación de términos como aviso de privacidad, dato público, sensible, así como su

transferencia y transmisión, lo cual es de suma importancia ya que busca realizar una distinción entre el tratamiento del dato en los límites del territorio como fuera de él.

Otra de las novedades del citado decreto es la obligación que impone a todas las empresas, sea públicas o privadas, a proveer una descripción detallada de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de la información, lo cual es concordante con el Artículo 21, literal a de la Ley 1581 de 2012.

Así mismo, se incorporaron las formas de obtener autorización y de revocar, así como la manera en la que deben ser tratados los datos personales de niños, niñas y adolescentes, que por regla general se encuentran prohibidos, pero como excepción se establece que los mismos son sujetos de tratamiento cuanto son de carácter público, para lo cual se debe cumplir con los siguientes requisitos: a) Que responda y respete el interés de los niños, niñas y adolescentes; b) Que se asegure el respeto de sus derechos fundamentales. En la actualidad, si bien es cierto los esfuerzos han sido bastantes, se carece de medidas que fortalezcan el régimen colombiano, respecto del uso, transmisión y recolección de datos por medio de diferentes plataformas electrónicas y sistemas informáticos que han sido desarrollados con diferentes propósitos.

Unión Europea

La Unión Europea (anteriormente Comunidad Económica Europea) fue pionera con un importante desarrollo respecto de legislación enfocada a la protección de datos personales como un derecho de todo ciudadano, para ello en 1981 se creó la primera norma internacional denominada "*Convenio 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento de datos con carácter personal*" pero que fue quedando obsoleta frente a los cambios en la forma en que se obtenían, almacenaban y procesaban los datos.

Para el año 1995, producto de múltiples esfuerzos se migró a la Directiva 95/46/CE del Parlamento Europeo y del Consejo que se aprobó el 24 de octubre de 1995, dando un gran paso respecto de la protección de las personas físicas, así como a la libre circulación de dicha información, así como la adopción de medidas para el flujo transfronterizo de data entre los países integrantes de la comunidad, hoy Unión Europea.

Posteriormente, el Reglamento General de Protección de Datos, de ahora en adelante GDPR, fue adoptado el 27 de abril de 2016 y tras un periodo de aplicación de dos años entró en vigor el 25 de mayo de 2018, el cual regula y establece Leyes para el tratamiento de datos personales teniendo en cuenta el crecimiento de las nuevas tecnologías que hace susceptibles a las personas a exponerse a un tratamiento indebido de sus datos personales. Con esta norma se pretendió, no solo, la protección de datos personales, sino también la apropiada y correcta integración de datos de una forma homogénea entre los países miembros, tal como lo menciona Torres Llanten (2020).

Con esta norma la Unión Europea busca garantizar el derecho fundamental a la protección de datos, consagrado en la Carta de los Derechos Fundamentales de la Unión Europea[2] y en los Tratados base de la unión, (artículo 16 del Tratado de Funcionamiento de la Unión Europea, en adelante, el «TFUE»). Según la Comisión Europea, a través del GDPR se reforzaron las salvaguardias de protección de datos, se aportaron a los particulares derechos adicionales y más sólidos, una mayor transparencia, y se garantizó que todos aquellos que tratan datos personales en el ámbito de su aplicación deban rendir más cuentas y tengan una mayor responsabilidad; así mismo se otorgó a las autoridades independientes de protección de datos competencias mayores y

[2] Carta de los Derechos Fundamentales de la Unión Europea, articulo 8:

armonizadas e implanta un nuevo sistema de gobernanza. Igualmente, según la Comisión Europea se crearon unas condiciones de competencia equitativas para todas las empresas que operan en el mercado de la UE, con independencia del lugar en el que estén establecidas, y se garantizó la libre circulación de datos dentro de la UE, reforzando así el mercado interior (Comunicación de la Comisión al Parlamento Europeo y al Consejo - La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos, 2020).

Dentro de los resultados del informe anteriormente citado de aplicación de dicho reglamento resaltan, el establecimiento de un sistema de gobernanza innovador, basado en autoridades independientes de protección de datos de los Estados miembros, la cooperación en asuntos transfronterizos y la creación del Comité Europeo de Protección de Datos. En igual sentido, los particulares son cada vez más conscientes de sus derechos: de acceso, rectificación, supresión y portabilidad de sus datos personales, de oposición al tratamiento y una mayor transparencia. El GDPR ha fortalecido los derechos procesales, incluyendo el derecho a presentar una reclamación ante una autoridad de protección de datos y el derecho a la tutela judicial, lo que deja entrever los grandes avances que presenta la Unión Europea en la adopción de medidas tendientes a la protección de los datos personales, no solo dentro de su territorio, sino de organizaciones que aun estando fuera de la unión recopilan información que pudiese llegar a ser sensible acorde a los postulados del GDPR.

Por lo anterior, el GDPR surge como una respuesta a los constantes cambios y desafíos, que hoy en día se tienen respecto a la protección de datos con la implementación de nuevas tecnologías de la información, la internet y la gestión de datos en grandes volúmenes, buscando salvaguardar los intereses de los habitantes de dicha comunidad.

CAPÍTULO II. COMPARATIVO EN RELACIÓN CON LAS DISPSICIONES GENERALES

En menester ahora hacer un comparativo entre las dos legislaciones sobre protección de datos, para lo cual se tomarán los principales ejes en que se centran las normas para ir adelantando de manera paulatina el análisis.

El objeto y ámbito de aplicación

Las disposiciones colombiana y europea comparten el objeto por el cual las normatividades fueron expedidas, ambas en la búsqueda de la protección de los datos personales de las personas físicas. En la ley colombiana se especifica aquellos verbos rectores que hacen parte de la protección, a saber, conocer, actualizar y rectificar (Ley 1581 – Articulo 1). Seguidamente las disposiciones legales relacionan esa protección a la garantía de los derechos fundamentales y libertades, haciendo una referencia implícita al derecho de *habeas data*, reconocido en la Declaración Universal de Derechos Humanos (Constitución Política de Colombia – Articulo 15, en conexidad con la Declaración de Derechos Humanos – Articulo 12) y a la autodeterminación informativa, la cual le permite al individuo decidir qué datos o no pueden ser conocidos, previa su autorización expresa.

En el ámbito de aplicación de la ley y el reglamento europeo va destinado al tratamiento de los datos personales registrados en cualquier base de datos, aunque la aplicación en el ámbito europeo expresa que el reglamento se extiende al tratamiento automatizado y no automatizado, lo cual demuestra que es una protección completa a cualquier operación que se haga con los datos personales por parte del responsable del tratamiento (artículos 2 y 3 del GDPR).

Igualmente, en las normas se mencionan las excepciones de aplicabilidad de la ley o del reglamento. En términos generales, ambas regulaciones no aplican para los datos que son utilizados en actividades personales o domésticas y para aquellos datos que son de uso de autoridades competentes por temas de seguridad y defensa nacional (artículos 16 y 18 del GDPR y Articulo 2 de la Ley 1581 de 2012). Cabe resaltar que la legislación colombiana también excluye aquellas bases de datos y de archivos que son parte de la actividad periodística, puesto su actividad está protegida por vía constitucional, y la información que se obtiene por el secreto profesional, además de aquellas bases de datos que son protegidas y reguladas por leyes especiales, como la Ley 1266 de 2008 que regula la protección de datos en actividad financiera, crediticia, comercial y de servicios y la Ley 79 de 1993 que regula la información sobre el censo poblacional y de vivienda.

Principios

La Ley 1581 de 2012 en su artículo 4, establece los principios por los cuales se interpretará y aplicará la norma, en total son ocho, a diferencia de los seis principios previstos en la regulación europea.

Como principio fundamental está la legalidad, el cual es de suma importancia en la relación entre el Estado y el individuo. En razón a ello, la Corte Constitucional en sentencia C-710 de 2001 cuyo magistrado Ponente fue Jaime Córdoba estableció de manera genérica sobre este principio que:

> "[…] Y de otro lado, define la relación entre el individuo y el Estado al prescribir que el uso del poder de coerción será legítimo solamente si está previamente autorizado por la

> Ley. Nadie podrá ser juzgado sino conforme a las Leyes preexistentes al acto que se le imputa".

En adición, esta corporación desarrollo este principio en la sentencia C-282 de 2011, cuyo magistrado ponente fue Alejandro Linares Cantillo, que:"

> […] El Legislador estatutario se encuentra facultado para definir los derechos y deberes de la fuente y el operador del tratamiento de datos, siempre que sus mandatos sean claros y acordes al principio de legalidad. Sobre este aspecto, la jurisprudencia constitucional ha precisado que es competencia del Legislador estatutario regular (i) las condiciones en que los titulares pueden acceder a la información difundida sobre ellos; (ii) la carga de veracidad y actualización sobre la información que comparten los bancos de datos, y en general, las reglas que deben seguir las entidades financieras para garantizar la actualización de la información; y (iii) las regulaciones sectoriales y generales del derecho, que prevén los principios, reglas, definiciones, derechos y deberes de los actores involucrados en la administración de datos, peticiones, reclamos, quejas y sanciones".

El principio de finalidad es similar en ambas legislaciones, las cuales prevén que el uso de los datos personales debe asegurarse para fines determinados, explícitos y legítimos que requieren la autorización de su titular. Sobre este particular la Corte Constitucional colombiana en la sentencia C-748 de 2011, señaló que el principio de finalidad implica un ámbito temporal, es decir, que el periodo de conservación de los datos personales no puede exceder el tiempo necesario para alcanzar la necesidad por la cual fueron registrados. Y un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas. (Sentencia C-748/11, 2011). A diferencia de la regulación colombiana la aplicabilidad del principio de finalidad está expreso en la regulación europea, en su artículo 5, numeral 1 – subsección b, el cual guarda

similitud con el marco normativo colombiano en lo que respecta al amito material y temporal, como en su momento lo expreso la Corte Constitucional en la ya citada sentencia.

Así mismo, la regulación europea contempla el principio de exactitud, a partir del cual se despliega el derecho a la actualización y rectificación de datos por parte del titular y exige que se desarrollen todas las medidas necesarias para que dichas rectificaciones se realicen sin dilación alguna. El responsable del tratamiento de los datos debe vigilar que los datos sean correctos, completos y estén actualizados (artículos 5 – Literal d y 16 del General Data Protection Regulation GDPR).

En este mismo sentir, la legislación colombiana establece el principio de veracidad o calidad, que vislumbra la misma visión del derecho de exactitud promulgado por el GDPR. Según El principio de veracidad, los datos personales deben obedecer a situaciones reales, actualizadas y comprobables y el principio de integridad de datos el cual prohíbe que los datos sean incompletos y puedan inducir al error (artículos 5 – Literal f del General Data Protection Regulation GDPR y Articulo 4 – Literal d de la Ley 1581 de 2012).

El principio de libertad que se expresa en la Ley colombiana se sustenta en la libertad que tiene el titular de entregar y divulgar sus datos personales, previo consentimiento expreso e informado. En este sentido la Corte Constitucional ha señalado que

> […] Este principio le permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente". (Sentencia C-748/11, 2011)

Igualmente aparece enunciado el principio de transparencia, el cual consiste en el derecho que les asiste a los titulares de la información sobre la forma en la que son tratados sus datos y la información que reposa en las bases de datos de los controladores o encargados. En este punto es preciso afirmar que el principio de transparencia es más desarrollado en la legislación colombiana que en la europea, toda vez que dentro del GDPR el mismo solo es abordado dentro del articulo 5 y 12, estableciendo parámetros generales para que los responsables del tratamiento informen a los titulares de la información de los datos que se encuentran almacenados, mientras que en la Ley 1581 de 2012, se profundiza en un aspecto importante como lo es la forma en la que se está procesando la información, los métodos empleados y los contactos de responsables y encargados, lo que le permite al titular el acceso en cualquier momento a la información que sobre el mismo este en una base de datos o archivo. Sin embargo, la Corte Constitucional ha referido que el encargado o responsable del tratamiento de los datos debe ofrecer como mínimo la siguiente información:

> […] i). información sobre el controlador de datos; ii). el propósito del procesamiento de los datos; iii). a quien se le pueden revelar los datos; iv). Como el titular de datos afectado puede ejercer cualquier derecho revisto en la norma y v). cualquier otra información para el tratamiento justo de los datos". (Sentencia C-748/11, 2011)

La legislación europea si bien no es extensa en la descripción del principio de transparencia, en el momento de su aplicación y materialización lo incorpora como el primer derecho de titular de datos, y advierte que el responsable del tratamiento de datos debe tomar las medidas oportunas para facilitar al titular toda la información relacionada a sus datos cuando dicha información ha sido entregada o no por el mismo (artículo 12 del General Data Protection Regulation GDPR). Cualquier comunicación sobre el tratamiento de datos personales debe otorgarse de forma concisa,

transparente, de fácil acceso, con un lenguaje sencillo y claro en especial toda aquella información que esté dirigida a menores de edad, por lo anterior es menester evitar el abuso en el uso de citas legales, o de términos anfibológicos (artículos 13 y 60 del General Data Protection Regulation GDPR).

Asimismo, impone al responsable del tratamiento de datos la obligación de facilitar al interesado la información relativa a sus datos previa solicitud, sin dilación indebida, dentro del mes desde el momento en que se presentó la solicitud por parte del titular, término que se podrá prorrogar por otros dos meses. La información se puede facilitar por escrito, medios electrónicos o verbalmente, de ser necesario será posible solicitar la acreditación de identidad del interesado.

En cuanto al principio de acceso y circulación restringida, este consiste en la obligación que se les impone a los individuos que recolectan información respecto al tratamiento, por lo que este, deberá efectuarse de conformidad con la autorización otorgada por el titular, así como su disponibilidad, lo que implica que no podrá ser divulgada de forma pública si esto no se encuentra dentro del consentimiento otorgado por cada individuo en particular. De acuerdo con lo anterior, la ley colombiana establece que los límites al tratamiento de datos están otorgados por los mimos titulares y por la ley, es decir, solo podrán hacer uso de los datos personales del titular, aquella persona a la cual este le hubiese otorgado autorización y aquellas personas que prevé la ley.

Asimismo, la norma se debe interpretar en el entendido que se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, a menos que exista autorización legal expresa (artículo 4 Ley 1581 de 2012). Por otro lado, el manejo de la información que no es publica, debe realizarse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella, de lo contrario, el responsable y el encargado del tratamiento de los datos serán responsables de los perjuicios causados el titular.

La norma europea no contempla una circulación restringida de los datos personas dentro de su territorio, por el contrario, la circulación de datos es libre, siempre y cuando se cumplan con las especificaciones que la ley establece tanto para responsable como para el encargado de la protección de los dados (artículo 3 del General Data Protection Regulation GDPR)

El principio de seguridad, el cual, según Navarro (2008) , se ha convertido en un elemento indispensable y necesario para seguir avanzando en esa carrera sin fin previsible de los países (p. 290), está contemplado de forma independiente en el artículo 32 de la regulación europea, en este se hace una explicación extensa sobre las medidas técnicas u organizativas que deben aplicar el responsable y encargado del tratamiento de datos. Estas medidas deben contener: la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas de tratamiento, la capacidad de restaurar la disponibilidad y acceso a los datos personales ante un incidente físico o técnico y un proceso de verificación y evaluación de la eficacia de las medidas técnicas y organizativas. Además, en la norma europea este principio está inmerso en el principio de integridad y confidencialidad, mediante el cual los datos personales serán tratados de manera que se garantice la seguridad adecuada, incluyendo la protección contra el tratamiento no autorizado o ilícito y su perdida, destrucción o daño accidental, por medio de la aplicación de medidas técnicas u organizativas apropiadas.

En Colombia la aplicación del principio de seguridad está determinado de forma similar a lo previsto en la Unión Europea, otorgándole la responsabilidad de la seguridad de los datos al responsable o encargado del tratamiento de datos personales, pero no se establecen los estándares mínimos que deben contener las medidas organizativas

> "[…] el responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. ¨ […] Existe entonces un deber tanto de los responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria" (Sentencia C-748/11, 2011)

El ultimo principio que prevé la Ley 1581 de 2012, es el principio de confidencialidad, el cual predica que toda persona que interviene el tratamiento de datos personales que no sea de naturaleza pública, están obligados a garantizar la reserva de la información, aun cuando ya hayan terminado su relación con las labores que comprenden el tratamiento, en la norma europea como se estableció previamente está contemplada la confidencialidad con el tratamiento seguro de los datos a través de las medidas técnicas y organizativas desarrolladas por el responsable y el encargada del tratamiento de datos.

Ahora bien, dentro del GDPR de la Unión Europea se hace referencia al principio de limitación del término de conservación de datos, por medio del cual se establece que no es posible mantener los datos del titular por más tiempo del necesario para el fin requerido, y solo se podrán conservan durante plazos más largos siempre que se trate exclusivamente con fines de archivo de interés público, investigación científica o histórica o estadísticos, sin que por ello se vulnere los derechos y libertades del titular (artículo 5 – Literales b y e del General Data Protection Regulation GDPR).

En Colombia, este principio no está determinado de forma expresa, sin embargo, el Decreto 1074 de 2015 por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio,

Industria y Turismos en su artículo 2.2.2.25.2.8, establece las limitaciones temporales al tratamiento de los datos personales, así:

> […] Artículo 2.2.2.25.2.8. Limitaciones temporales al Tratamiento de los datos personales. Los responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión. No obstante, lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.” (Decreto 1074 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, 2015)

Como novedad, la regulación europea introduce en sus principios la responsabilidad proactiva, también conocida como *accountability*. Este principio, según la Escuela de privacidad (2020) establece que es obligación del responsable de tratamiento de datos, la aplicación de medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento de datos personales es conforme con el reglamento (pp 14-15). Para ello, la misma regulación desarrolla medidas obligatorias que den cumplimento con este principio, dentro de las cuales se tiene: la figura del delegado de protección de datos, las medidas de protección desde el diseño y por defecto, el registro de las actividades de tratamiento y análisis del riesgo, las medidas técnicas y organizativas de seguridad, la notificación de quiebras de seguridad, entre otras.

El desarrollo de estas medidas y de aquellas adicionales que puedan implementar los responsables y encargados del tratamiento de datos les permitirá otorgar el *accountability* del tratamiento de datos y así garantizar los derechos y libertades que tiene los titulares de sus datos personales. El fin de este principio es que todas aquellas personas involucradas en el tratamiento de datos aseguren una actitud consciente, diligente y proactiva para el manejo de los datos y de su seguridad.

En la legislación colombiana no está el concepto general de la responsabilidad proactiva, la Ley 1581 no establece este concepto. Empero, el Decreto 1074 de 2015, prevé la responsabilidad demostrada frente al tratamiento de datos personales, y para ello solicita que los responsables del tratamiento de datos deben estar en la capacidad de demostrar ante la Superintendencia de Industria y Comercio, que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones de la Ley estatutaria, al respecto solo establece la demostración en la naturaleza jurídica del responsable, la naturaleza de los datos personales objeto de tratamiento, el tipo de tratamiento, los riesgos potenciales, descripción de los procedimientos implementados y evidencia de la implementación efectiva. (Decreto 1074 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, 2015)

Es claro que la norma no hace referencia a demostrar de forma expresa las medidas de seguridad aplicadas por el responsable para el tratamiento de datos en caso de tratamiento no autorizado, perdida, destrucción o daño accidental, lo cual deja en desventaja los derechos de los titulares, puesto que solo impone un requisito a nivel administrativo básico, pero que no impone una responsabilidad que desarrolle, como si lo hace la unión europea, una actitud consciente, diligente y proactiva del responsable y encargado del tratamiento de datos.

Licitud del Tratamiento de Datos Personales

El artículo 6 de la regulación europea dispone los supuestos en los cuales es licito el tratamiento de datos y los describe así: cuando existe un consentimiento del titular para uno o varios fines específicos, para la ejecución de un contrato en el que el titular es parte o la aplicación de medidas precontractuales, para el cumplimento de una obligación legal aplicable al responsable del tratamiento, para proteger intereses vitales del titular o de otra persona física, para el cumplimento de una misión realizada en interés público o en ejercicio de poderes públicos conferido al responsable del tratamiento y para la satisfacción de intereses legítimos perseguidos por el responsable de datos personales o un tercero, siempre y cuando no prevalezcan los intereses o derechos y libertades fundamentales del interesado que requiera la protección de sus datos personales, en particular si es un niño.

En relación con el consentimiento, la norma en el considerando numero 32 refiere que "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" Articulo 4, numeral 11 del General Data Protection Regulation GDPR). Por lo cual, este consentimiento debe estar marcado por la voluntad efectiva del titular de los datos, si el consentimiento del titular está viciado de alguna duda en su origen será ilícito el tratamiento de sus datos, no puede existir la posibilidad de obtener consentimiento tácito o con pre – autorizaciones no explicitas.

También será licito en la ejecución de contrato, esto hace referencia a los datos personales que son necesario en el perfeccionamiento de contratos laborales, civiles o administrativos y en los cuales debe existir la plena seguridad de confidencialidad e integridad cuando el tratamiento

es por una obligación legal que es aplicable al responsable de tratamiento de datos, cabe la posibilidad que el titular de estos pueda hacer prevaler sus derechos y libertades y ejercer el derecho de oposición contemplado en la norma europea. Empero, será aplicable la licitud del tratamiento si el responsable o encargado, puede demostrar que el tratamiento en deber legal se presentó por prevención de fraude, trasmisión de datos dentro del mismo grupo empresarial y la trasmisión de datos para garantizar la seguridad de las redes. (Considerando 75 y artículo 6 del General Data Protection Regulation GDPR)

Cuando el tratamiento de datos se necesita para cumplir una obligación legal o una misión realizada en interés público, la finalidad del tratamiento deberá quedar determinada en la base jurídica, es decir en casos taxativos, y que serán de manejo por cada uno de los Estados miembros, pero que deberán contener como mínimo, la condiciones generales que rigen la licitud del tratamiento, los tipos de datos objeto de tratamiento, los titulares afectados, la entidades a las cuales se le puede comunicar los datos, y los fines de dicha comunicaciones, los plazos de conservación de los datos y las operaciones y procedimientos del tratamiento. (Artículo 6, sub-numeral 3 – literal b del General Data Protection Regulation GDPR)

En Colombia la Ley estatutaria establece cinco supuestos para licitud del tratamiento de datos personales. A diferencia del reglamento europeo, en Colombia se requiere la autorización explicita del tratamiento por parte del titular salvo excepciones legales que no establezcan dicha autorización. La autorización debe ser previa, expresa e informada, según las definiciones de ley. Al respecto la Corte Constitucional expresó:

> […] “La Sala considera que, de conformidad con el principio de libertad, es posible que las personas naturales den su consentimiento, por su puesto, expreso e informado, para que sus datos personales sean sometidos a tratamiento. En estos casos deberán cumplirse con

> todos los principios que rigen el tratamiento de datos personales, en especial cobrará importancia el principio de finalidad, según el cual el dato sensible solamente podrá ser tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional." (Sentencia C-748/11, 2011)

Como la ley estatutaria no reglamentó los procesos o medidas para la consecución de la autorización, el Decreto 1074 en su artículo 2.2.2.25.2.2, consigna que será el responsable del tratamiento de datos quien debe adoptar los procedimientos necesario para solicitar la autorización al titular, a más tardar en el mismo momento de recolección de los datos y deberá informarle que datos son necesarios y las finalidades específicas para el tratamiento de estos. Adicionalmente, concordante con el artículo 2.2.2.25.2.4, del ya mencionado Decreto, los mecanismos para obtener la autorización también serán de elección del responsable del tratamiento de datos y se entenderá que existió la autorización, si es por escrito, de forma oral, o mediante conducta inequívocas del titular que permitan concluir de forma razonable que otorga la autorización, pero aclara que el silencio no es una conducta inequívoca, lo anterior debe conservarse como prueba de la autorización del titular de los datos.

Finalmente, el decreto instituye que el titular de los datos puede revocar o suprimir la autorización previamente otorgada en cualquier momento, y deberá realizarlo a través del reclamo, cuya herramienta será desarrollada por parte del responsable o encargado del tratamiento de datos y deberá ser gratuita y de fácil acceso.

El segundo supuesto está dirigido a la licitud del tratamiento para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado, en tal evento los representantes legales son quienes deben otorgar esta autorización. El interés vital, está relacionado con las afectaciones graves frente a la salud y la vida del titular, si el titular está dentro

de esta condición es lícito hacer uso de sus datos personales. Ahora bien, si el titular tiene algún tipo de incapacidad legal o física, la licitud del uso de sus datos estará en manos de obtener la autorización previa del representante legal, quien se presume es el guardián de los intereses del titular

El tercer supuesto establece que el tratamiento sea efectuado en el curso de actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical y se referirá exclusivamente a sus miembros o las personas que mantengan contacto regular con estas. En concordancia con el principio de libertad, se exige que cualquier suministro de datos terceros debe estar precedida obligatoriamente por la autorización expresa del titular.

El cuarto supuesto de uso licito de datos tiene que ver con aquellos datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, al respecto la Corte Constitucional, en la sentencia C-748 de 2011, lo ejemplificó de la siguiente manera:

> […]los datos sensibles (de las partes, los testigos y otros intervinientes) en muchos procesos judiciales son indispensables para resolver una controversia; piénsese por ejemplo en un proceso de tutela sobre discriminación o en un proceso penal en el que una víctima reclama reparación por violaciones a sus derechos como consecuencia de una persecución política o religiosa. En estos casos los datos sensibles deben ser puestos en conocimiento de la respectiva autoridad judicial no solamente para resolver la controversia, sino incluso para la adopción de medidas de protección.” (Sentencia C-748/11, 2011)

En virtud de los principios de finalidad, legalidad, confidencialidad y libertad, los datos para este supuesto requieren, el consentimiento expreso del titular, orden judicial cuando sea el

caso, prohibición del uso de los datos para propósito diferente al proceso judicial y la garantía que la autoridad judicial y los intervinientes en el proceso deben mantener en absoluta confidencialidad los datos suministrados.

El último supuesto está relacionado con el uso de datos cuya finalidad sea histórica, estadística o científica, pero se aclara que deben adoptarse medidas conducentes a la supresión de la identidad de los titulares, el uso de los datos será necesario para la reconstrucción historia, científica o estadística, puesto que contribuyen a mejor diseño de políticas públicas y del funcionamiento del estado, para la satisfacción de derechos fundamentales y principios constitucionales como la vida y la salud.

En suma, es posible determinar que los presupuestos de ambas normatividades son similares, sin embargo el reglamento adoptado por la de la Unión Europea es explícito en determinar que la licitud del uso de los datos está en cabeza de los responsables y encargado del tratamiento de datos personales y que su actividad se debe ajustar a estos presupuestos, a diferencia la ley colombiana que es más general y evita expresamente otorgar responsabilidad de licitud de uso de datos personales a los responsables y encargados del tratamiento, salvo en la normatividad que hace referencia a la autorización previa en donde es claro quiénes son responsables del desarrollo de las medidas y procedimientos para la obtención de dicha autorización. En consecuencia, la Ley 1581 de 2012, no se estipulan parámetros específicos para que los responsables y encargados ejecuten de forma licito el tratamiento en situaciones puntuales y tampoco se desarrollan excepciones, como por el ejemplo en caso de conductas fraudulentas, que les permitan a estos implementar un tratamiento tendiente a evitar que se consume tal conducta, lo que puede dejar sin herramientas que mitiguen los riesgos de manera proactiva e impidan que se

materialicen daños a los titulares, lo que en el largo plazo puede representar un desmedro en la calidad y fiabilidad de la información.

El consentimiento del titular de los datos

Dentro de los principios establecidos por el GDPR, se han definido seis circunstancias en las que se puede realizar el consentimiento, como lo regula el artículo 6 de la norma mencionada. En este sentido, el artículo 7 del reglamento se encarga de desarrollar las condiciones para que el consentimiento otorgado goce de plena validez para el tratamiento de los datos personales dentro de la Unión Europea, los cuales se procederán a detallar a continuación y a comparar con lo preceptuado por la Ley 1581 de 2012, el cual es el marco normativo colombiano análogo.

A. CONSENTIMIENTO PREVIO

Bajo el primer escenario, el controlador, quien es el encargado del procesamiento de los datos recopilados, tiene la obligación legal de demostrar que la persona otorgo de manera expresa y voluntaria el consentimiento para la ejecución de todas las actividades del tratamiento. Lo anterior, guarda estrecha relación con lo que reza el artículo 4 literal C de la Ley 1581 de 2021, ya que la base legal del tratamiento de datos en la legislación colombiana es el consentimiento previo, el cual está relacionado con el denominado principio de libertad, desarrollado mediante la sentencia C-748 de 2011. En la referida providencia, la Corte Constitucional proporciona una línea general, en lo que respecta a los requisitos para que se dé cumplimiento al principio de libertad, en los siguientes términos:

> […] De todo lo anterior, puede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, no está permitido el consentimiento tácito del Titular del dato y sólo podrá

> prescindirse de él por expreso mandato legal o por orden de autoridad judicial, (ii) el consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez". (Sentencia C-748/11, 2011)

En concordancia con lo anterior, hace una precisión importante esta corporación en lo que respecta a que el consentimiento del titular debe ser libre, previo, expreso e informado y bajo ningún caso deberá iniciar el tratamiento de los datos, mediante la aplicación de la figura de consentimiento tácito, la cual alude a esas acciones u omisiones que den a entender que se autoriza el tratamiento. De modo similar el GDPR, dentro de sus considerandos menciona lo siguiente:

> "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. […] Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta" (Considerando 32 General Data Protection Regulation GDPR)

Llama la atención, que a diferencia de la normativa colombiana se fijan parámetros adicionales al otorgamiento del consentimiento y la forma en la que puede realizase, por lo que surge la especificidad, como característica propia para la concesión de la autorización de los datos y el carácter inequívoco, en cuanto a la no admisión de múltiples interpretaciones y el grado de facilidad de comprensión para las personas. En adición, respecto a los medios, los cuales pueden ser físicos y digitales, como a bien lo establece el reglamento, deben garantizar su conservación en caso de requerimiento legal o del usuario propietario de la información, lo que guarda estrecha relación con la autorización que realiza el titular del dato a la luz de la Ley 1581 de 2012 en su artículo 9 y las formas de obtención de la autorización fijadas en el artículo 2.2.2.25.2.4. del Decreto 1074 de 2015.

Finalmente, es importante el desarrollo que de manera ejemplificante detalla el reglamento europeo, en cuanto al uso de formularios preestablecidos o formularios de cara a informar por medios electrónicos a los usuarios la manera en que será ejecutado el tratamiento y recolección, al igual que las excepciones que no constituyen el otorgamiento de consentimiento como lo son el silencio, las casillas ya marcadas o la inacción, lo que en debidas proporciones, se asemeja a la figura de consentimiento tácito desarrollado en la sentencia C-748 de 2011.

B. CONSENTIMIENTO PARA TRATAMIENTO DE MANERA CONCOMITANTE CON OTROS ASUNTOS:

Se refiere al otorgamiento del consentimiento que se proporciona de manera simultánea a la celebración de un contrato, por ejemplo, en donde se recopila información personal sujeta a tratamiento legal, en este punto encontramos una de las principales diferencias de la norma europea con respecto a la norma colombiana que carece de clausulado sobre el asunto, por lo que al tenor del numeral 1 del artículo 7 del GDPR se estipula:

Artículo 7:

[…] Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiere a otros asuntos, la solicitud de consentimiento se presentará de una manera que se distinga claramente de los demás asuntos, de forma inteligible y fácilmente accesible, utilizando y lenguaje sencillo. cualquier parte de dicha declaración que constituya una infracción del presente Reglamento no será vinculante.

y

4. Al evaluar si el consentimiento se otorga libremente, se tendrá en cuenta en la mayor medida posible si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, está condicionada al consentimiento para el procesamiento de datos personales que no es necesario para la ejecución de ese contrato. (artículo 7, numerales 1 y 4 del General Data Protection Regulation GDPR)

En primer lugar, es necesario tener presente en este aspecto se debe dar cumplimiento a los parámetros previos para el consentimiento, pero se imponen dos obligaciones adicionales, respecto a la manera en la que se debe presentar el mismo y el grado de libertad con el que se realiza. En este orden de ideas, en caso de que se esté autorizando el tratamiento de datos, será necesario que la solicitud sea de fácil distinción para el otorgante al momento de la autorización. Por otra parte, la libertad del consentimiento no deberá verse alterada respecto del negocio o los otros asuntos que se están discutiendo. No será un consentimiento libre si el interesado no tiene una elección genuina o libre o no puede rechazar o retirar el consentimiento sin perjuicio para este, de acuerdo con el artículo 42 del reglamento europeo. Y es que al incorporarse a las condiciones generales del contrato surgen dos riesgos, en primer lugar, que las autorizaciones se camuflen en el resto del contenido del contrato, y en segundo lugar que para el titular de los datos sea imposible escindir

entre la aceptación del contrato y la posibilidad de decidir si autoriza el uso de los datos de manera libre y consciente.

Llama la atención este punto, pues en Colombia, con la utilización de los contratos de adhesión, regulados en la Ley 1480 de 2011 – artículo 5, la cual los define como "Aquel en el que las cláusulas son dispuestas por el productor o proveedor, de manera que el consumidor no puede modificarlas, ni puede hacer otra cosa que aceptarlas o rechazarlas" (Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones, 2011). Esta figura cuenta con cláusulas tipo para el tratamiento de datos personales, el consumidor y titular del dato, en últimas se ve abocado a la suscripción del misma so pena de no contar con el servicio o producto del que es objeto el negocio jurídico, lo que al tenor del reglamento europeo viciaría la libertad a saber. En el derecho colombiano podría pensarse en una vulneración al principio de la libertad, aunque no haya norma que se refiera a ese aspecto puntual.

C. RESPECTO DEL CONSENTIMIENTO EN CASO DE MENORES DE EDAD

Salta a la vista que mientras el GDPR considera el otorgamiento de este tipo de datos, como uno de los principios generales de la normativa, la Ley 1581 de 2012 inicialmente, no desarrolla este aspecto, aunque si establece los derechos a los cuales son acreedores los niños, niñas y adolescentes respecto del tratamiento de sus datos.

Respecto al otorgamiento del consentimiento, es necesario precisar que a la luz del artículo 8 del reglamento europeo, se considera niño de acuerdo con el apartado primero a la persona que tenga entre 13 y 16 años, por lo que es necesario que los controladores empleen mecanismos adecuados que les permitan conocer la edad de la persona que da su consentimiento a fin de no incurrir en el incumplimiento de la normativa. Se impone, además, que en caso de que se deban tratar datos de niños se requiere la autorización o consentimiento del tutor legal, de no contar con

esto, el tratamiento será considerado ilegal, por lo que el controlador debe efectuar esfuerzos razonables para validar tal autorización.

Si los servicios de información están dirigidos directamente a los niños, no sería aplicable esta disposición. Sin embargo, el consentimiento del tutor legal no afecta las disposiciones generales de derecho en relación con l validez y nulidad, aplicables a una relación contractual que surja con un menor de edad.

Ahora bien, como se mencionó en un principio la Ley 1581 no alude a la forma en que debe ser otorgado el consentimiento de los niños, ni qué edad comprende este concepto, por lo que es necesario acudir a artículo 3 de la Ley 1098 de 2006, que indica:

> […] Artículo 3°. Sujetos titulares de derechos. Para todos los efectos de esta Ley son sujetos titulares de derechos todas las personas menores de 18 años. Sin perjuicio de lo establecido en el artículo 34 del Código Civil, se entiende por niño o niña las personas entre los 0 y los 12 años, y por adolescente las personas entre 12 y 18 años de edad. (Ley 906 de 2004 - Por la cual se expide el Código de Procedimiento Penal, 2004)

Realizada dicha precisión para Colombia, mediante el Decreto 1074 de 2015 en el artículo 2.2.2.25.2.9, el cual desarrolla el artículo 7 de la Ley 1581 de 2021 se indica que deberá contarse con la debida autorización del representante legal del niño, niña o adolescente de forma previa al inicio del tratamiento, pero que a su vez este podrá ser escuchado y su opinión será valorada bajo los criterios de madurez, autonomía y capacidad para entender el asunto.

En principio, la norma colombiana proporciona un mayor margen de protección en lo que respecta a la edad de los menores, al igual que les concede autonomía y autodeterminación en consideración al asunto en donde se otorgue el consentimiento, pero deja vacíos importantes respecto a la manera en que se obtiene y valida la información con el propósito de validar la edad

de quien proporciona datos sujetos a tratamiento, abordaje que sí efectúa el reglamento europeo. Tampoco se analiza o se impone el deber de validación, respecto a determinar si la persona que avala el consentimiento del niño, niña o adolescente es verdaderamente su tutor o representante legal, creando una brecha importante respecto al grado de confiabilidad y validez de dicho consentimiento.

D. RETIRO DEL CONSENTIMIENTO

Una vez otorgado el consentimiento para el tratamiento de los datos, el titular tiene el derecho y puede revocar el mismo, siendo este uno de los escenarios en donde se presenta una marcada diferencia entre las dos regulaciones objeto de estudio. Así las cosas, la Ley 1581 de 2012 en su artículo 8, donde se abordan los derechos de los titulares, plantea en el numeral e:

> Articulo 8
>
> […]e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a esta Ley y a la Constitución;" (Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales, 2012).

De lo anterior se infiere que en la actualidad en el sistema de protección de datos colombiano la revocación de la autorización de tratamiento de datos se da bajo dos presupuestos, los cuales se encuentran plasmados en la Resolución número 35093 de 2020, donde se menciona que:

> (i) no se respeten los principios, derechos y garantías constitucionales y legales. En este caso, y en aras de garantizar el debido proceso, siempre y cuando la Superintendencia de

> Industria y Comercio haya determinado que en el Tratamiento el responsable o encargado han incurrido en conductas contrarias al ordenamiento y (ii) en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos. (Superintendencia de Industria y Comercio, 2020)

A su paso, el GDPR menciona que el interesado tiene derecho a retirar su consentimiento en cualquier momento y que el proceso para tales efectos gozara de la misma facilidad que al momento del otorgamiento. A diferencia del régimen jurídico colombiano, dentro del marco europeo se da total discrecionalidad al titular de la información al momento de la cancelación de los permisos otorgados para su tratamiento, bien sea que medie o no obligación legal o contractual que impida que su revocación, como ocurre si según la Ley 1581 de 2012 y los postulados formulados en la sentencia C-784 de 2011. Adicionalmente y según el análisis efectuado por vía jurisprudencial por Chaljub (2011), en el territorio colombiano se reviste de la misma facultad, es decir la de revocación, a la Superintendencia de Industria y Comercio, posterior a que dicho órgano haya determinado flagrantes violaciones por parte del encargado del tratamiento que afecten los principios, derechos y garantías constitucionales y legales. (Sentencia C-748/11)

Datos sensibles y su tratamiento

De acuerdo con el Título III, articulo 5 de la Ley 1581 de 2012, constituyen datos sensibles, “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías

de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos". La Superintendencia de Industria y Comercio ha destacado la importancia de esta clase de datos personales, según la entidad: "La definición de dato sensible no está solamente relacionada con la garantía propia del ejercicio del derecho de habeas data, sino que también va ligado al derecho fundamental a la intimidad, el cual igualmente, es sujeto de protección constitucional" (Superintendencia de Industria y Comercio, 2018.). Nótese que en documentos como la historia clínica de una persona (López Oliva, Vargas Chaves & Alarcón Peña, 2022) los datos sensibles pueden ser susceptibles de sex expuestos en clara vulneración del derecho fundamental al habeas data.

Así mismo, la SIC, ha mencionado que:

> Se trata entonces de una especie de datos con mayor rango de protección frente a los otros datos como lo son los privados, los semiprivados y los públicos, según la categorización que hace la norma colombiana. Hacen parte de este grupo en Colombia los datos biométricos según ha precisado la entidad (Superintendencia de Industria y Comercio, 2018)

En este sentido el GDPR define dentro del artículo 9, que dichos datos son aquellos de carácter:

> "personal que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin de identificar de forma única a una persona física, datos relacionados con la salud o datos relacionados con una persona la vida u orientación sexuales de la persona". (artículo 9 del General Data Protection Regulation GDPR)

Una vez definido que existen notables similitudes en cuanto lo que abarca el concepto de datos sensibles, se hace imperioso analizar la forma de tratamiento dentro de cada una de las legislaciones.

Tabla 1.

Régimen de excepciones al tratamiento de datos sensibles

EXCEPCIÓN	LEY 1581 De 2012	GDPR
Consentimiento explícito	Tanto la Ley 1581 De 2012 como el GDPR encuentran que una de las excepciones para el tratamiento de los datos sensibles, encuentra fundamento legal en el consentimiento otorgado de manera previa, según los parámetros abordados con anterioridad en el presente escrito.	
Necesarios a los efectos del cumplimiento de las obligaciones y el ejercicio de derechos específicos en el ámbito de la legislación laboral y de la seguridad social	No hace alusión	Aclara que deberán estar previstos en documento donde conste relación laboral
Necesario para la protección de los intereses vitales del interesado o de otra persona física cuando el interesado no pueda dar su consentimiento	Al respecto se considera necesario que los representantes legales deberán otorgar su autorización.	Como cláusula de exclusión menciona que el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física.

En el curso de actividades legítimas con las debidas garantías por una fundación, asociación o cualquier otro organismo sin fines de lucro con un objetivo político, filosófico, religioso o sindical.	Ambas legislaciones contemplan esta excepción respecto del tratamiento de los datos contenidos en el artículo 6 literal c de la Ley 1581 de 2012 y Articulo 9 literal d del GDPR.	
Relacionado con los datos personales que el interesado ha hecho públicos de forma manifiesta	No contemplado	Alude a datos que se hacen públicos manifiestamente. Es necesario determinar que para que exista esa notoriedad el titular de los datos debe "hacer públicos los datos afirmativamente y conocer el resultado de dicha publicidad. La mera existencia en el espacio público no entra en el plazo de publicación en este sentido" (GDPRHub. 2020)
Necesario para el establecimiento, ejercicio o defensa de reclamos legales o siempre que los tribunales actúen en su capacidad judicial	Ambas legislaciones contemplan esta excepción respecto del tratamiento de los datos contenidos en el artículo 6 literal d de la Ley 1581 de 2012 y Articulo 9 literal e del GDPR.	
Necesario por motivos de interés público sustancial, sobre la base de la legislación de la Unión o del Estado miembro	Permite el procesamiento de categorías especiales de datos cuando hay un interés público sustancial involucrado. El tratamiento se llevará a cabo sobre la base de la legislación de la Unión o de los Estados miembros, y será proporcionado al objetivo perseguido, respetará la esencia del derecho a la	

	protección de datos y preverá medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses del interesado. (GDPRHub. 2020)	
Necesario para fines medicinales o para la gestión de sistemas y servicios de salud	No contemplado	Los fines medicinales comprenden la medicina preventiva u ocupacional, la evaluación de la capacidad de trabajo del empleado o el diagnóstico médico. La gestión de los sistemas de salud incluye la prestación de atención o tratamiento sanitario o social y la gestión de los sistemas y servicios de atención sanitaria o social. Requiere la existencia de un contrato con un profesional de la salud e impone como condición complementaria: los datos serán tratados por o bajo la responsabilidad de un profesional sujeto a la obligación de secreto profesional. (GDPRHub. 2020)
Necesario por motivos de interés público en el ámbito de la salud pública	No contemplado	Procesamiento de datos personales con el objetivo de proteger contra amenazas transfronterizas graves para la salud o garantizar altos estándares de calidad y seguridad de la atención médica y de los medicamentos o dispositivos

		médicos. Esto debe hacerse sobre la base de la legislación de la Unión o de los Estados miembros, que prevé medidas adecuadas y específicas para salvaguardar los derechos y libertades del interesado, en particular el secreto profesional. (GDPRHub. 2020)
Necesario para archivar nuestros fines en el interés público, fines de investigación científica o histórica o fines estadístico	Ambas legislaciones contemplan esta excepción respecto del tratamiento de los datos contenidos en el artículo 6 literal e de la Ley 1581 de 2012 y Articulo 9 literal j del GDPR.	

Nota: esta tabla ilustra las principales diferencias y similitudes existentes entre Régimen de excepciones al tratamiento de datos sensibles (fuente: elaboración propia).

Como se aprecia, el reglamento europeo implementa figuras novedosas respecto al tratamiento de datos sensibles por razones de interés y salud pública, seguridad nacional y servicios de salud, los cuales hoy en día Colombia no tiene legislados con suficiente detalle. Finalmente, el reglamento de la Unión Europea permite que los Estados miembros de acuerdo con su legislación interna adicionen cláusulas para el tratamiento de datos genéticos, biométricos o aquellos relacionados con la salud.

Falencias regulatorias de la Ley 1581 De 2012 respecto de los principios establecidos en el GDPR

Una vez efectuado el comparativo de las regulaciones en lo relativo a los principios y aspectos base, se proceder a identificar las principales falencias regulatorias que se observan en la legislación colombiana en la materia.

A. RESPECTO DEL TRATAMIENTO DE DATOS PENALES

Efectuada la revisión de los principios generales del GDPR, respecto de la Ley 1581 de 2012, se encuentra un vacío normativo en lo que respecta al tratamiento de datos personales relacionados con condenas y procesos penales.

Partiendo del hecho que las personas inmersas dentro de un proceso penal y durante el desarrollo del mismo se ven expuestas a revelar datos personales que permiten su individualización e identificación, de acuerdo con lo establecido en el Código de Procedimiento Penal, Ley 906 de 2004, artículos 288 y 337, esta información en muchas ocasiones es de conocimiento público, materia que no ha sido regulada por el legislador, pero que por vía de desarrollo jurisprudencial la Corte Constitucional que refiere:

> [---] en sentencias como la T-414 de 1992 y T-729 de 2002 considera que los antecedentes penales son datos personales en la medida en que, asocian una situación determinada (haber sido condenado, por la comisión de un delito, en un proceso penal, por una autoridad judicial competente) con una persona natural. Estos datos personales son propios y exclusivos de la persona, y permiten identificarla, reconocerla o singularizarla en mayor o menor medida, de forma individual o en conexión con otros datos personales" (Sentencia SU-458/12, 2012)

En esta misma vía, la Corte Constitucional mediante sentencia T-020 de 2014 realizó las siguientes precisiones:

> [---] Si bien los antecedentes constan en un documento público, dicha información no tiene esa misma naturaleza, pues más allá de identificar, reconocer o singularizar –en mayor o menor medida– a una persona, como ocurre con cualquier dato personal, en virtud de los mandatos previstos en la Constitución, que apuntan a proteger el derecho al trabajo (CP art. 25), a identificar a la pena con un fin resocializador (CP art. 34) y adoptar medidas que

> impidan la discriminación o exclusión social (CP art. 13), se entiende que, por los efectos negativos que le son propios, es inadmisible su acceso o divulgación general o ilimitada. Precisamente, este tipo de datos permiten asociar y vincular el nombre de una persona con acontecimientos no queridos, perjudiciales o socialmente reprochables, que conducen al debilitamiento de una imagen o incluso a la dificultad de poder construir una en el futuro (Sentencia T-020/14, 2014)

Y en lo que respecta a las sentencias proferidas por el órgano jurisdiccional afirmo:

> *Aun cuando se entiende que las sentencias son públicas, y así deben seguir siéndolo, la información personal contenida en ellas está sometida a los principios de la administración de datos, por lo que eventualmente pueden incluir datos sensibles o semiprivados, en cuya circulación y acceso deben cumplirse los principios de finalidad, necesidad y circulación restringida que rigen el derecho al habeas data*. (Sentencia T-020/14, 2014)

Revisten de importancia los pronunciamientos de la Corte Constitucional en la medida en que dan una línea general respecto al tratamiento de los datos personales, en observancia del postulado del artículo 15 constitucional, pues se hacen las siguientes precisiones:

- Determinar que el tratamiento de los datos personales referentes a la ejecución de penas requiere especial cuidado por parte del Estado y las entidades competentes, ello habida consideración a que la información contenida en los documentos públicos, por medio de los cuales se impone la pena y/o medida de seguridad, tienen inmersos datos de carácter semi privados que pueden permitir la identificación y/o relación de la persona y en su momento la eventual exclusión al darse el proceso de reinserción a la sociedad.

- Al contener información que solo le interesa a un grupo determinado de personas, los datos plasmados en las sentencias proferidas por el aparato jurisdiccional se catalogan como datos semiprivados, por lo que se deberá garantizar su adecuado tratamiento.

En contraste la normativa de la Unión Europea, en su artículo 10 desarrolla la manera en la que deben tratarse este tipo de datos. En primera medida le asigna el tratamiento de manera exclusiva a la autoridad oficial competente, pero impone la carga respecto del tratamiento con el fin de que se respeten los derechos y libertades de la persona. El Tribunal de Justicia Europeo ha planteado pautas generales para la concesión de anonimato total o parcial de las partes dentro de un proceso judicial, lo que requiere seguir las siguientes reglas:

1. Si una parte estima necesario que en un asunto sometido al Tribunal General no se divulgue públicamente su identidad, deberá dirigirse al Tribunal con arreglo al artículo 66 del Reglamento de Procedimiento para que, en su caso, este imponga el anonimato, total o parcial, en el asunto de que se trate.
2. La solicitud de anonimato deberá presentarse mediante escrito separado debidamente motivado.
3. Para que el anonimato sea eficaz, es necesario presentar dicha solicitud desde el inicio del procedimiento. A causa de la difusión en Internet de la información relativa al asunto, la utilidad de la decisión de imponer el anonimato resulta comprometida si ya se ha mencionado el asunto de que se trate en la lista de asuntos sometidos al Tribunal General que se publica en el sitio web del Tribunal de Justicia de la Unión Europea o cuando ya se haya publicado en el Diario Oficial de la Unión Europea la comunicación relativa al asunto de que se trate.» (Concesión del anonimato a las partes en los procedimientos judiciales

ante el Tribunal General de la Unión Europea, p.1, 2019)

Así las cosas, se observa como en el territorio colombiano, el tratamiento de datos personales asociados a procesos de índole penal, no tienen una regulación expresa en la Ley 1581 de 2012, por lo que, los titulares de los mismos se han visto avocados a recurrir a la acción de tutela , para que por medio de dicho mecanismos se garantice el derecho fundamental del habeas data, siendo esto una figura desarrollada por el legislador negativo, lo que sin duda plantea una mayor congestión para el aparato judicial y que requiere a toda luz pautas claras, definidas por ejemplo sea por un Decreto reglamentario, que le permitan a los jueces una correcta aplicación del derecho.

Respecto del procesamiento que no requiere identificación

El artículo 11 del reglamento europeo identifica dos situaciones, a saber, la primera donde el procesamiento por parte del controlador no requiere la identificación del titular de los datos, lo cual va de la mano con los principios de anonimización de los datos y necesidad, por lo que el controlador no debe iniciar la recopilación de información a tratar y deberá, según Aguirre (2018) "contar con 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, y que 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" (p. 89).

La segunda situación radica en que, al no poder identificar al titular de los datos, se excluye la aplicación de los artículos 15 al 20 del reglamento, fijando como excepción, cuando la persona

proporcione información adicional al controlador que permita su identificación, obligando al controlador a demostrar la imposibilidad de identificación. Podría entonces llegar a pensarse, de manera errada que lo anterior guarda similitud con el principio de finalidad establecido en el artículo 4 literal b de la Ley 1581 de 2012, pero es importante realizar las siguientes acotaciones:

- Tal principio se limita a mencionar que el tratamiento debe obedecer a una finalidad legitima de acuerdo con la constitución y la Ley.
- Por desarrollo jurisprudencial, la Corte Constitucional en diferentes pronunciamientos, como por ejemplo las sentencias C-748 de 2011 precisa que:

> […]la finalidad no sólo debe ser legítima, sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular y que el principio de finalidad implica también: (i) un ámbito temporal, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.” (Sentencia C-748/11, 2011)

Por lo anterior, es correcto afirmar que mientras el reglamento europeo hace alusión al procesamiento de datos donde no sea posible identificar a su titular, la legislación colombiana no menciona dicha práctica ni impone cargas al respecto al responsable o encargado del tratamiento en este aspecto puntual. En consecuencia, la Ley 1581 de 2012, no incorpora técnicas como por ejemplo la anonimización, adición de ruido y/o métodos similares, que impidan la plena identificación de los titulares de los datos, lo que eventualmente podría generar fallos considerables en lo que respecta a fugas de información, fiabilidad e integridad de los datos, por mencionar algunos. Nótese en este punto que, por vía jurisprudencial, únicamente se alude a la

finalidad de la recolección, haciendo hincapié en el propósito de la recolección y los tiempos de conservación de la información, pero no de las medidas de seguridad necesarias para que dicha labor garantice unos mínimos de anonimización.

CAPÍTULO III. DERECHOS DE LOS TITULARES DE LA PROTECCIÓN DE DATOS.

A continuación, se compararán las normativas, en lo atinente a los derechos básicos de mayor relevancia de los titulares de los datos que deben ser garantizados por las autoridades, en cada uno de los territorios, por lo que se procederá a examinarlos.

Transparencia, Presupuestos para su aplicación

Dentro de los presupuestos del GDPR se encuentra a la luz del artículo 12, el tratamiento de la información de forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. A continuación, se procede a realizar el análisis de cada uno de estos aspectos:

a. *Concisión:* se refiere a la manera en la que debe presentarse la información, con el propósito de evitar que se suministren datos que no sean relevantes o que guarden relación con el tratamiento de datos.

b. *Transparencia:* busca es que el titular de los datos esté en la capacidad de determinar de manera anticipada, el alcance y la forma en la que serán procesados los datos que serán suministrados. Dentro de este concepto, se incluye la información que deber ser entregada al titular de la información referente a la forma en que se recopila la información, el destino de esta y la manera en que será tratada y dispuesta de acuerdo con la finalidad por la que se recopila, lo cual va de la mano con el otorgamiento previo del consentimiento.

c. *Inteligibilidad:* significa que la información debe ser comprensible para un miembro promedio de la audiencia destinataria. Un controlador de datos responsable tendrá conocimiento sobre el tipo de personas sobre las que recopila información y con dicho conocimiento determina lo que normalmente entendería dicha población objetivo.

Ahora bien, con el fin de que los controladores puedan tener completa seguridad respecto del grado de compresión y transparencia de la información y la efectividad de las interfaces de usuario, avisos, políticas, y demás mecanismos empleados para la recolección de información, será necesario que efectúen pruebas que permitan tener certeza respecto del cumplimiento de la normativa.

d. Formularios de fácil acceso: El interesado no debería tener que buscar la información, esta debe ser evidente y de fácil acceso a los usuarios. Es necesario que el responsable del tratamiento proporcione la información directamente a los interesados, vinculándolos a ella, o señalizándola claramente.

e. *Lenguaje claro y sencillo:* mediante la implementación de información escrita, o en los casos cuando la información se transmita oralmente o por audio, se deben emplear las mejores prácticas para una comunicación clara y oportuna. Con este requisito se busca que los datos que se proporcionen sean entregados de forma sencilla, evitando el uso de estructuras sintácticas complejas que puedan transmitir un mensaje errado al usuario.

Concordante con lo anterior, dentro del artículo 12 del GDPR se establecen como formas de información, no solo la suministrada mediante medios escritos, sino que se introduce una figura novedosa dentro del reglamento que consiste en iconos estandarizados, los cuales ofrecen una visión de conjunto del tratamiento previsto. El diseño de estos iconos deberá hacerlo la Comisión Europea, que ya está trabajando para presentar una propuesta (de Datos, 2020).

Igualmente, se establece que los iconos deberán ser claros y limitados, es decir, cuantos más iconos aparezcan más difícil será para el interesado entender el significado de estos. Por lo cual, se recomienda realizar pruebas con los usuarios para ver si los iconos que se pretenden utilizar permiten una comprensión fácil y clara por parte del usuario (de Datos, 2020b).

Asimismo, el artículo contempla la utilización de medios electrónicos, sitios web y la utilización de botones emergentes, avisos y similares para poner de presente a los titulares de la información la recolección de datos, que debe ser adaptado, para sitios web donde los destinatarios son infantes, haciendo necesario el uso de recursos didácticos y que capten la atención de esta población.

Finalmente, contempla de forma específica que la información se puede proporcionar oralmente a un interesado que lo solicite, siempre que su identidad se demuestre por otros medios. En otras palabras, los medios empleados más que basarse en una mera afirmación por parte del individuo de que es una persona específica, deben permitir al responsable del tratamiento verificar la identidad de un interesado con suficiente certeza (GDPRHub, 2020).

Por el contrario, se evidencia un sucinto desarrollo de la legislación colombiana al respecto, únicamente aborda el tema de la transparencia en el artículo 4 de la Ley 1581 de 2011, aludiendo a la no imposición de restricciones respecto de la información que solicite el titular de los datos, sin enfatizar de forma clara y contundente las medidas de transparencia a implementar por parte de los responsables y encargados del tratamiento.

Información y acceso a los datos personales

Al respecto resulta importante precisar que la información y su acceso, consiste en la facultad que ostenta el titular de la información a solicitar los datos que se encuentran en posesión

y/o administración por parte de un controlador y/o responsable, en cualquier tiempo y lugar y sin dilación alguna.

Es necesario tener en cuenta que dentro del GDPR se hace una distinción importante en cuanto a la recopilación de datos de manera directa o indirecta. Aún con esta diferenciación, las disposiciones generales en cuanto a estructura y contenido guardan uniformidad, asimismo constituyen un medio probatorio para que el interesado pueda determinar de manera previa el grado, alcance y consecuencias del tratamiento que se realizara.

Dicho lo anterior, el reglamento de la Unión Europea no dejó a discrecionalidad de los controladores la información que es de obligatorio cumplimiento para el tratamiento, la cual debe proporcionarse de manera previa a la obtención de los datos personales, los cuales serán abordados a continuación:

a. *Identidad y datos de contacto del responsable del tratamiento:* esta información es un requisito previo para que el interesado pueda ponerse en contacto con el responsable del tratamiento y ejercer su derecho a la información y al acceso cuando sea necesario. Es ideal que el encargado pueda proporcionar datos de contacto, con la finalidad de que las personas puedan tener un mecanismo de contacto con el responsable del tratamiento. Algunos encargados, en lugar de proporcionar directamente al interesado sus datos de contacto ofrecen en su lugar un formulario de contacto en línea. Para poder enviar dicho formulario de contacto, el interesado generalmente debe completar algunos campos obligatorios, como el nombre, la dirección de correo electrónico o la naturaleza de la solicitud. Si bien algunos formularios de contacto requieren una información mínima y, por lo tanto, facilitan que el interesado se ponga en contacto con el responsable del tratamiento, otros pueden requerir información específica, como un inicio de sesión, una

identificación de cliente o un número de contrato, que no todos los interesados tienen, lo que lo hace imposible en la práctica el contacto con el encargado. (GDPRHub, 2020)

b. *Datos de contacto del delegado de protección de datos:* En algunos casos el responsable del tratamiento debe designar un delegado de protección de datos que tiene la obligación de supervisar las actividades de tratamiento realizadas por el responsable y actuar como punto de contacto para los interesados. Los datos de contacto del responsable del tratamiento deben incluir información que permita a los interesados contactarlo de forma sencilla. Esto puede incluir una dirección postal, un número de teléfono exclusivo y/o una dirección de correo electrónico dedicada.

c. *Finalidades y fundamento jurídico:* El artículo 13, apartado 1, literal c), establece que los responsables del tratamiento deben proporcionar los fines para los que se tratan los datos personales, así como la base jurídica correspondiente. La base legal debe encontrarse necesariamente en el consentimiento y debe adecuarse cuando se procesen categorías especiales de datos personales. Esto impone una carga a los controladores para identificar las diferentes bases legales en las que se fundamentan para procesar los datos personales y vincularlas con el fin del procesamiento.

d. *Interés legítimo:* Comprender el interés legítimo del responsable del tratamiento puede considerarse un requisito previo para que un interesado pueda ejercer otros derechos, como el derecho a oponerse al tratamiento. Con esta información, el interesado puede valorar si el interés invocado por el responsable del tratamiento es realmente legítimo y si el tratamiento es proporcionado, teniendo en cuenta el objetivo perseguido por el responsable del tratamiento y el impacto que puede tener sobre sus propios derechos e intereses.

e. *Destinatarios:* entendida como cualquier persona física o jurídica, lo que significa que deben estar cubiertas tanto las personas internas como externas, ya sean empleados, agentes o proveedores de servicios externos del controlador. En un aviso de privacidad dirigido a los empleados de una empresa, por ejemplo, deben identificarse todos los destinatarios de los datos del empleado, como el gerente de RR.HH. de esa empresa o un proveedor externo de servicios de nómina. Si no es posible identificar a todos los destinatarios (ya sea porque su identidad puede cambiar con regularidad o porque la lista sería abrumadoramente larga), los responsables del tratamiento deberían al menos identificar las categorías de destinatarios de los datos personales (GDPRHub, 2020).

En relación con lo anterior, la Ley 1581 la cual regula la protección de datos y su tratamiento no establece los ítems que se abordaron anteriormente, lo que implica que en muchas ocasiones cuando los usuarios entregan sus datos para el respectivo tratamiento, no se tenga claro el objetivo y finalidad del tratamiento y permite que los datos, terminando en diferentes compañías para temas completamente diferente por los cuales fueron inicialmente proporcionados. Ahora bien, la normativa colombiana en el artículo 12 de la ya citada Ley, establece como deber del responsable del tratamiento informar datos como el tratamiento al cual será sometida la información, los derechos de los titulares, la identificación, dirección física o electrónica y teléfono del responsable del tratamiento y el carácter facultativo para emitir respuestas cuando versen sobre datos sensibles de menores de edad.

Rectificación y supresión

Los derechos de rectificación y supresión se encuentran en los artículos 16 y 17 del GDPR de la Unión Europea respectivamente. Sin embargo, estos derechos se ven reforzados, en el reglamento con la adición de la limitación del uso de los datos y el derecho al olvido.

El derecho a la rectificación hace referencia a la posibilidad que tiene el titular de los datos a enmendar aquellos datos inexactos que el responsable tenga acerca del interesado, quien puede completarlo si el objeto del tratamiento lo requiere. De acuerdo con lo escrito por Dolores Martínez, este tipo derechos le otorga al titular el poder de disposición y control de sus datos personales, siendo estos de diferente contenido a aquellos derechos de intimidad y privacidad. (Martínez-Martínez, 2018). Este derecho ya venía contemplado desde la directiva 95-46 CE y en el nuevo reglamento no cambia su descripción.

En la regulación colombiana el derecho de rectificación tiene fundamento constitución a través del articulo 15 y se encuentra expreso en la Ley 1581 del 2012, el cual no difiere sustantivamente del derecho de la regulación europea, puesto que al igual que esta última, la regulación colombiana le otorga al titular de los datos la faculta de conocer, actualizar y rectificar los datos personales que sobre este existen en una base de datos o archivo.

Al respecto la Corte Constitucional expresó:

> "En efecto, el artículo 15 de la Constitución Política señala que "En la recolección, tratamiento y circulación de datos se respetaran la libertad y demás garantías consagradas en la Constitución." El hábeas data confiere en palabras de la Corporación "según la norma constitucional citada, un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información". Este control, no sólo se predica de la autorización previa para el Tratamiento del dato, **sino que el individuo también es libre**

> **de decidir cuales informaciones desea que continúen y cuáles deben sean excluidas de una fuente de información**, siempre y cuando no exista un mandato legal que le imponga tal deber, o cuando exista alguna obligación contractual entre la persona y el controlador de datos, que haga necesaria la permanencia del dato" (Sentencia C-748/11, 2011) (negrilla fuera del texto).

El derecho de supresión, de la reglamentación europea está referido como el derecho al olvido, y hace énfasis en la facultad que tiene el interesado de suprimir los datos personales que le conciernen, cuando se presente alguna de las siguiente situaciones: los datos personales ya no sean necesarios para el fin por el cual fueron recogidos, el interesado retire el consentimiento o se oponga al tratamiento de los mismo, los datos personales fueron tratado ilícitamente y la supresión de los datos se deba realizar por menester de la ley. Asimismo, cuando los datos por motivo alguno se hayan hecho públicos.

El derecho al olvido le otorga el poder a cada individuo de decidir sobre la facilidad o imposibilidad de acceso de sus propios datos de carácter personal, enmarcándose en la dignidad y libertad personal de cada ser y el respeto a su vida privada e intimidad (López-Sáez, 2017). En el ámbito europeo este derecho es de gran importancia, puesto que las situaciones descritas afectan en gran medida el ámbito digital, en el cual el derecho al olvido le permite al titular de los datos solicitar la supresión de su huella digital al responsable del tratamiento.

El mayor control de los datos personales proporcionado por el derecho al olvido digital tiene como finalidad, en última instancia, permitir a la persona desarrollarse libremente. Tal y como apunta parte de la doctrina, la construcción de la propia identidad o personalidad debe estar libre de restricciones13, garantizando el control de aquellos datos de carácter personal proporcionados de manera directa y consciente, así como aquellas huellas dispersas y proyectadas en el seno de la

World Wide Web. Así, se concibe el derecho al olvido digital, como nuevo derecho, vinculado al derecho fundamental a la protección de datos y enfrentado con las libertades de información. *(Ibidem, pag. 145)*

El derecho al olvido digital es entendido como aquel que le permite al titular borrar, ocultar e incluso cancelar todos los datos personales que de su pasado que le puedan afectar su desarrollo futuro, puesto que la realidad de la red, la información que se encuentra en línea puede perpetuar los datos allí consignados. Su ejercicio supone una tensión entre la libertad de información y la protección de datos personales (Manzanero y Pérez, 2016). Este derecho es relevante en al ámbito europeo, puesto que el mismo reglamento le impone al responsable del tratamiento la obligación de suprimir cualquier enlace a esos datos personales o cualquier copia o replica mediante las medidas técnicas disponibles. Es preciso aclara que el derecho al olvido no es absoluto, ni automático, contrario sensu, el reglamento europeo ha determinado limitantes al dicho derecho.

En Colombia, el derecho al olvido si bien esta consagra en la Ley estatutaria, se encuentra limitado a la manifestación de la Superintendencia de Industria y Comercio, la cual determina si en el tratamiento de los datos el responsable o encargado ha incurrido en conductas ilegales o contraria al a Constitución, después de reclamo enviado por el titular. En referencia al derecho de olvido en el ámbito digital, la Ley no expresa una protección en esta materia. De acuerdo con la investigación realizado por Galvis Cano y Salazar Bautista, el derecho al olvido es una figura que se evidencia como una facultad accesoria, la cual, si bien se ha buscado en iniciativas ante el Congreso que se reglamente como un derecho autónomo, su desenlace no sido el más favorable, puesto que algunos honorables senadores estiman que este derecho puede ir en contra de la libertad de prensa convirtiéndose en una forma de censura. (Galvis Cano & Salazar Bautista, 2018). Para que se garantice el derecho al olvido en el ámbito digital es necesario que, en el ordenamiento

jurídico colombiano, se realice un análisis en conjunto de este derecho con otros derechos que la Corte Constitucional mediante varios pronunciamientos ha garantizado; como el derecho al buen nombre, a la honra a la libertad de información y a la intimidad.

Otro de los derechos que se encuentra dentro del espectro de la rectificación y supresión, es el derecho de portabilidad de los datos personales, el cual figura en el artículo 20 del reglamento europeo y que le permite al interesado recibir por parte del responsable del tratamiento, la información que le ha suministrado, en un formato estructurado de uso común y lectura mecánica, para que se puede lo pueda transmitir a otro responsable, siempre y cuando exista el consentimiento claro, previo y expreso del uso de datos personales y se efectué por medios automatizados.

El derecho de portabilidad tiene un precursor muy conocido en la Unión Europea con la telefonía móvil, que permite el derecho de portabilidad numérica, sin embargo, con el avance tecnológico el derecho de la portabilidad también ya es un hecho con la información personal y por lo cual para el reglamento europeo era de suma importancia su regulación. Según el artículo 29 *working party*[3], la portabilidad de datos puede llevar a las empresas y a los usuarios o consumidores a maximizar los beneficios de la *big data* de una manera más balanceada y transparente. También puede ayudar a minimizar prácticas discriminatorias e injustas que reduzcan el riesgo del uso de datos inadecuados para la toma de decisiones, lo cual beneficia tanto a las empresas como a los usuarios o consumidores (Article 29 Data Protection Working Party, 2013).

[3]El articulo 29 Working Party (Art. 29 WP), cuyo nombre completo es "Grupo de Trabajo sobre la Protección de los Individuos en relación con el Procesamiento de Datos" fue un cuerpo administrativo compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor de Protección de Datos en Europa y la Comisión Europea. El propósito de este Grupo de Trabajo fue crear el articulo 29 de la Directiva de Proteccion de datos (Directiva 95/46/EC) promulgada en 1996, el cual fue reemplazado por la Junta de Protección de Datos el 25 de mayo de 2018 en concordancia con la Regulación General de Protección de Datos de la UE (RGDP 2016/679)

En la lectura del derecho de portabilidad se pueden analizar tres diferentes facultades que se le otorgan al titular de los datos. I). el derecho a recibir los datos que fueron suministrados; II). El derecho a transmitir los datos a otro encargado y III). El derecho de transmitir los datos personales de un encargado a otro. Estas tres facultades facilitan la interoperabilidad, resultado esperado a través de la aplicación del formato estructurado, de uso común y de lectura mecánica. Según la directiva 2013/37/EU un archivo estructurado de forma de lectura mecánica, es aquel que las aplicaciones de software puedan fácilmente identificar, reconocer y extraer datos específicos de este. La interoperabilidad, no es sinónimo de compatibilidad, por el contrario, es la habilidad de diversas y diferenciadas organizaciones tienen de interactuar para conseguir benéficos mutuos y objetivos en común, lo que incluye compartir información y conocimiento entre las organizaciones, a través de procesos de negocios entre sus respectivos sistemas de TIC (De Hertab et al., 2018).

En nuestro país, el derecho de la portabilidad aún se encuentra limitado a la portabilidad numérica, asunto este que es regulado por la Comisión de Regulación de Comunicaciones CRC y no es de competencia de la Superintendencia de Industria y Comercio regula y su delegatura para la protección de datos. Sobre este aspecto sólo existen las recomendaciones de la Red Iberoamericana de Protección de datos, de la cual Colombia, a través de la Superintendencia de Industria y Comercio hace parte, sus decisiones y recomendaciones no son vinculantes en el ámbito nacional.

Derecho de oposición y decisiones individuales automatizadas

El derecho de oposición, de acuerdo con la regulación europea, hace referencia a la facultad que tiene el titular, en cualquier momento y por motivos relacionados a su situación particular, a

oponerse a que datos personales sean objeto de tratamiento, caso en el cual, el responsable dejará de tratar los datos a menos que se acredite motivos legítimos imperiosos que prevalezca sobre los intereses, derechos y libertades del titular. Al respecto cabe anotar que este derecho hace parte de los llamados ARCO (acceso, rectificación, cancelación y oposición), lo cuales son la base fundamental para la garantía del derecho de habeas data. La normativa actual no ha generado por ello un cambio radical desde lo previsto en la directiva 95/46/CE4.

Al respecto la Agencia Española de Protección de Datos expresa que las personas tienen el derecho de oposición, para evitar la difusión pública que, de sus datos personales, hacen los buscadores a partir de fuentes de acceso público, que pueden generar un efecto negativo permanente en contra de la voluntad de los afectados (Reigada, 2012). Sin embargo, esto ha sido en la práctica una dificultad para muchos responsables del tratamiento, toda vez, que no es posible que este tenga un control sobre los datos que terceros puedan tener por enlaces, copias o réplicas de los web masters que se producen en internet.

Por lo anterior si bien el derecho de oposición puede ser alegado, el instrumento más eficaz seria como se vio previamente el derecho al olvido digital, puesto que le asegura el titular de los datos personales la posibilidad de borrar de forma definitiva su huella digital.

[4] Directiva 95/46/CE, Sección VII, Artículo 14 Derecho de oposición del interesado: Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización. Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

En Colombia, el derecho de oposición esta intrínseco en el numeral E del artículo 8 de la Ley estatuaria de habeas data, en el cual la acción del titular del dato personal se encuentra limitada por (i) que no se respeten los principios, derechos y garantías constitucionales y legales y (ii) siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o encargado han incurrido en conductas contrarias a esta Ley y a la Constitución. Sobre estas limitaciones, en el examen constitucional que se realizó a la Ley, se expresaba que estas, previo el consentimiento del titular, repercutían en que el titular perdiera indirectamente la titularidad del dato y con ello se limitara el derecho a la autodeterminación informática (Sentencia C-748/11, 2011).

Al respecto la Corte ha señalado que el derecho de habeas data le otorga al titular de los datos personales, la facultad de exigirle a quienes hagan el tratamiento de estos datos, el acceso, la exclusión, la corrección, la adición, la actualización y certificación de los datos, así como la limitación en la divulgación de los mismos, de conformidad con los principios que regula el proceso de administración de datos personales, en consecuencia:

> "el literal e) debe ser entendido en el sentido que el Titular podrá revocar la autorización y solicitar la supresión del dato cuando: (i) no se respeten los principios, derechos y garantías constitucionales y legales. En este caso, y en aras de garantizar el debido proceso, siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento y (ii) en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos." (Sentencia C 748 de 2011, Pág. 229)

Ahora bien, dentro de los derechos que la GDPR de la Unión Europea les garantiza a los titulares de los mismos, también están las decisiones individuales automatizadas, que de acuerdo con el artículo 22 de esta reglamentación, hace referencia a que el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluyendo perfiles, que produzcan efectos jurídicos en él o le afecte significativamente de modo similar. Una decisión automatizada es aquella que se realiza por medios tecnológicos sin la necesidad de la intervención del ser humano. Lo datos que se utilizan, pueden provenir de una diversidad de fuentes y las decisiones pueden llevarse a cabo con o sin la elaboración de perfiles. Los sectores en donde se hace mayor uso de este perfilamiento automatizado son el sector bancario y financiero, el sector de seguros, el publicitario y el de asistencia sanitaria. Las decisiones automatizadas tienen amplia aplicación comercial, toda vez que ofrecen mayor eficiencia y ahorro en recursos, pero pueden implicar riesgos importantes en los derechos y libertades de los titulares de datos personales si no se adoptan las garantías adecuadas (Gestiona Abogados, 2019).

Para la materialización de este derecho en la práctica, los encargados y responsables de tratamiento de datos han encontrado desafíos que con la directiva anterior no se preveían, puesto que este derecho incluye un ámbito mucho más específico de aplicabilidad, pero con conceptos jurídico más indeterminados. Por lo anterior, para valorar si una empresa está en concordancia con lo reglamentado en el artículo 22, el responsable del tratamiento deberá analizar si el objeto de este se encuadra en lo preceptuado por la reglamentación general y exigirá, de igual manera, la previsión de bases legales más restringidas para legitimar el tratamiento y un decálogo de facultades especificas en favor de los titulares de datos ante situaciones dudosas de aplicación.

Hoy en día la mayoría de las decisiones que toman las organizaciones, no son del todo automatizadas, generalmente el resultado que indica el algoritmo es utilizado como soporte para

que el ser humano tome una u otra decisión. Empero, la eficiencia de los algoritmos en la toma de decisiones ha vuelto cada vez más irrelevante la intervención humana. Por lo anterior, para que el encargado de la protección de datos no transgreda el derecho del artículo 22, la intervención humana debe ser significativa, debiendo existir una participación real de la persona en la decisión que le ha arrojado el programa informático, siendo esta característica, un elemento esencial para determinar o no si la decisión es automatizada. Para saber si la decisión automatizada genera efectos jurídicos o similares, es el responsable del tratamiento quien debe valorar si el concreto tratamiento que está llevando a cabo y la decisión que se deriva de este tratamiento, puede generar efectos significativos en el titular de los datos, y, asimismo, al responsable le corresponde establecer criterios objetivos que le permitan decidir si tal tratamiento genera los efectos indicados (Ortigosa, 2019).

En el caso colombiano, la Ley 1581 del 2012 o el Decreto 1074 de 2015, no estable un derecho para que el titular de datos pueda ejercer los derechos básicos ARCO en razón al uso de los datos personales por decisiones automatizadas, de acuerdo con la cita hecha extraída por Ana María Trujillo en relación con la protección de datos por decisiones automatizadas:

> *La legislación colombiana debe imponer restricciones y garantías en la toma de decisiones automatizadas y en la creación de perfiles. Sectores de la doctrina consideran que la aproximación más apropiada para regular estos como tratamiento de datos personales es consolidar el derecho a no ser objeto de estos cuando puedan tener consecuencias para las personas y afectar sus derechos. Para asegurar una mayor protección, es importante que el precepto normativo imponga una prohibición de someter a las personas a decisiones automatizadas y/o perfiles, salvo determinadas excepciones (*Sentencia C-748/11, 2011).

Resulta pues, imperioso que en Colombia se regule este tipo de decisiones, esto por las eventuales implicaciones que podría generar para los titulares de los datos, al ser un hecho generador de derechos y obligaciones, que de alguna forma no estarían siendo asumidas de forma voluntaria y consciente por parte de los titulares, sino por herramientas algorítmicas diseñadas para tal fin.

CAPÍTULO IV. RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS.

El responsable del Tratamiento de Datos

El responsable del tratamiento de datos en el régimen normativo colombiano es la figura encargada de garantizar el cumplimiento de los parámetros referentes al tratamiento y protección de datos. En este sentido la Ley 1581 de 2012, lo define como "*Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos"*. *R*esulta importante detenerse en este punto, para ver cómo la legislación colombiana impone las obligaciones a la persona que realiza el tratamiento, ya sea, por sí mismo o por interpuesta persona.

En adición, el responsable dentro de la Ley 1581 de 2012 tiene el deber de conservar la información con estándares de seguridad que no permitan la manipulación, adulteración, sustracción de los datos por personas no autorizadas, garantizando su actualización y disponibilidad bajo la observancia del consentimiento otorgado por el titular de la información. Asimismo, se traslada la carga de la prueba, en la medida en que recae la responsabilidad sobre el responsable la conservación del respectivo consentimiento otorgado para el tratamiento.

Al respecto la Superintendencia de Industria y Comercio, ha desarrollado mediante guías lo atinente al principio de responsabilidad demostrada, el cual guarda estrecha relación con las responsabilidades que le asisten al responsable del tratamiento de los datos. Con el ánimo de abordar tal principio, resulta conveniente comprender que el objetivo es que las organizaciones que recopilan y realizan tratamiento de datos deben adoptar medidas tendientes al cumplimiento efectivo de los principios de privacidad y protección de datos. **(**de Industria y Comercio, 2014)

Acorde con lo anterior, el Decreto 1377 de 2013, en su artículo 27, fijo los parámetros que deberán tener en cuenta los responsables del tratamiento para definir las políticas internas, con las cuales se busca dar cumplimiento a las obligaciones que le son propias, acorde con el artículo 17 de la Ley 1851 de 2012, por lo que se deberá garantizar:

1. Existencia de una estructura administrativa proporcional a la estructura del responsable para implementarlas,

2. Adopción de mecanismos internos para poner en práctica las políticas que incluyan herramientas de implementación, entrenamiento y programas de educación, y

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

El objetivo es implementar dentro de las organizaciones modelos de gestión del riesgo, que como lo ha manifestado la Superintendencia de Industria y Comercio, deben incorporar políticas que respondan a los ciclos internos de gestión de datos dentro de la organización y que generen resultados medibles que les permitan poner a prueba el nivel de protección. **(**de Industria y Comercio, 2014)

Ahora bien, para que dichas políticas sean exitosas es menester que se cuente con el compromiso de la organización, a través de la adopción de una cultura de tratamiento de datos,

por lo cual la alta dirección jugará un papel importante en la socialización de dichas medidas y su adecuada implementación, apoyándose en el área encargada para proteger los datos con total disposición de los recursos y personal necesario para su aplicación.

Se deberá designar un oficial de protección de datos, esto según el artículo 23 del Decreto 1377 de 2013, quien asumirá la función de protección de datos personales, que dará trámite a las solicitudes de los titulares, así como la elaboración, administración, actualización, seguimiento y monitoreo del programa para la protección de datos.

Dentro de estos programas es importante implementar la identificación de riesgos asociados al tratamiento y con ello realizar monitoreo, y controles que disminuyan su impacto y probabilidad y puedan afectar a la organización ante eventuales materializaciones. La Guía para la implementación del principio de responsabilidad demostrada, sugiere las siguientes etapas:

1. Identificación: de los posibles riesgos a los cuales se ven expuestos los datos personales, para ello se deberá documentar procesos y procedimientos, definir metodologías de identificación de riesgos y su materialización.

2. Medición: evaluando su probabilidad de ocurrencia y su impacto.

3. Control: definidos como las acciones a adelantar para controlar o mitigar los riesgos inherentes al tratamiento de datos personales, se recomienda definir periodicidad y tipos.

4. Monitoreo: como el seguimiento constante al programa de riesgos definidos, con el ánimo de evaluar las medidas adoptadas en los pasos anteriores.

Como vemos, las políticas se enfocan en la gestión del riesgo como uno de los pilares fundamentales para la toma de decisiones de carácter preventivo que permitan cumplir con las obligaciones legales que les asisten a los responsables.

En este sentido el sistema colombiano no dista mucho del marco europeo, el cual en el artículo 24 del reglamento, impone igualmente la carga de la prueba sobre el responsable del tratamiento respecto a la conservación del consentimiento. Lo anterior va de la mano con el artículo 5, el cual impone al responsable del cumplimiento normativo y de demostrarlo, lo que se conoce en el ordenamiento europeo como la responsabilidad proactiva.

Al respecto, el GDPR indica la adopción de medidas, en el siguiente sentido:

1. Registro de Actividades.
2. Medidas de Protección de Datos desde el Diseño.
3. Medidas de Protección de Datos por Defecto.
4. Medidas de Seguridad Adecuadas.
5. Evaluaciones de Impacto.
6. Autorización previa o Consultas previas con la Autoridad de Control.
7. Delegado de Protección de Datos.
8. Notificación de Violación de Seguridad.

Acorde con la Agencia Española para la Protección de Datos (2021), se enuncia que

> […] la gestión del riesgo se da en dos vías, la primera de ellas enfocado en los derechos y libertades, la cual tiene por objetivo el estudio del impacto y la probabilidad de causar daño a las personas, a nivel individual o social, como consecuencia de un tratamiento de datos personales; y la segunda, que consiste en la gestión de riesgo de cumplimiento normativo que tiene por objetivo facilitar al responsable una herramienta para verificar el grado de cumplimiento de las obligaciones y preceptos exigidos legalmente con relación a una actividad de tratamiento. (p.19)

Otro de los puntos a resaltar dentro de la legislación europea, es que no solo se centra en el tratamiento de riesgos de forma correctiva, sino con carácter proactivo, la cual no se reduce a las consecuencias del riesgo sino a la manera de evitar su materialización. La única diferencia sustancial se encuentra como diferencia entre los tiempos para reportar brechas de seguridad, donde para el caso de la Unión Europea contará con 72 horas, según el considerando 85 del RGPD, mientras que en Colombia se cuenta hasta con 15 días hábiles, El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio. Finalmente, se puede decir que la legislación colombiana y la europea dan un enfoque al responsable del tratamiento de datos personales fundamentado en el riesgo y la definición de políticas adecuadas para su identificación, tratamiento, medición y control.

Protección de datos desde el diseño y por defecto

Es necesario, en primera medida entender que esta figura tiene su origen con el exponencial avance tecnológico, que inicio desde la década de los 90, en donde por primera vez se abordó la preocupación de la protección de los datos desde una perspectiva proactiva, tal como lo menciona Cavoukian (2009):

> "En este sentido, anticipa y evita eventos invasivos de privacidad antes de que sucedan. Por oposición, no espera a que se verifiquen los riesgos de privacidad, como tampoco supone soluciones por infracciones de privacidad una vez que han ocurrido. En síntesis, la PpD[5] viene antes del hecho, no después (p.13). En adición, resulta pertinente mencionar que el concepto de privacidad resulta ser algo hetero, acorde con Taylor (2012), quien

[5] Protección desde el diseño

menciona que el mismo es considerado en relación con "el interés público", por lo que juega un papel importante en el establecimiento de relaciones en esa misma esfera (p. 13)

Hecha la anterior precisión, es necesario mencionar que dentro del ordenamiento jurídico colombiano, a la fecha, no existe una figura igual o similar a la antes citada; la Superintendencia de Industria y Comercio, como órgano rector en esta materia, ha realizado un esfuerzo considerable con el ánimo de desarrollar esta figura, vinculándola con el principio de responsabilidad demostrada[6], por esto, se han expedido varias guías por este organismo[7], en las cuales se busca concienciar a los responsables del tratamiento de adoptar medidas tendientes a que el aseguramiento de la privacidad se convierta en el modo de operación predeterminado de una organización*"*[8].

En ese orden de ideas y de acuerdo con diferentes pronunciamientos de la Superintendencia de Industria y Comercio, se debe considerar como apropiadas las medidas en el sentido de que se deben considerar como mínimo los siguientes factores:

a. Nivel de riesgo

b. Naturaleza de los datos.

c. Consecuencias ante una eventual vulneración y la magnitud del daño que puede causar al titular.

d. Tamaño de la organización

[6] El principio de responsabilidad demostrada exige que los obligados del régimen de protección de datos adopten medidas apropiadas y efectivas para el cabal cumplimiento de las exigencias de la Ley 1581 de 2012 y Decretos reglamentarios. Mecanismos que deben ser acordes con el tamaño y estructura de la organización, que serán sujetos de verificación por la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio en cualquier momento

[7] Véase Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) o guía para la implementación del principio de responsabilidad demostrada En las transferencias internacionales de datos personales.

[8] Superintendencia de Industria y Comercio, Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales

e. Recursos disponibles

f. Estado de la técnica, y

g. Contexto y finalidades del tratamiento.

A contrario sensu, la regulación europea proporciona de manera expresa los lineamientos generales que se deben adoptar para la protección desde el diseño[9] teniendo un carácter vinculante; de esta manera al efectuar una revisión del artículo 25 del GDPR se alude a los factores mínimos que la SIC ha venido sugiriendo, aunque adiciona la puesta en marcha de técnicas como la seudonimización [10] para cumplir los principios de protección del dato, su minimización e integridad.

En la anonimización, se requiere que se suprima del dato los elementos suficientes que permiten la identificación del titular, como indica el Dictamen 05/2014 sobre técnicas de anonimización, que establece que para aplicar esta técnica "*hay que tratarlos de tal manera que no puedan usarse para identificar a una persona física mediante «el conjunto de los medios que puedan ser razonablemente utilizados» por el responsable del tratamiento o por terceros",* por lo anterior es posible inferir que:

a. Anonimizar los datos, impide la identificación del titular de manera permanente.

b. No existe una técnica regulada para realizar tal procedimiento, por lo que se deberá recurrir al estado del arte para tal efecto.

c. Existen riesgos asociados a la anonimización de la información.

[9] Para más información consultar "*the Opinion 5/2018 Preliminary Opinion on privacy by design"* o Accountability o "the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies Summary"
[10] Seudonimización, según Garcia y Pardo (2018), es aquella técnica, que oculta la identidad del titular de un dato, pero permite volver a identificarla en caso necesario. (p. 98)

Ahora bien, el Grupo de trabajo sobre Protección de las Personas de la Unión Europea en lo que respecta al tratamiento de datos personales ha realizado las siguientes criticas:

a. Anonimización permanente: teniendo en cuenta que el Tribunal de Justicia de la Unión Europea en su sentencia sobre el asunto College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer, impone una regla para la protección de los datos personales, en el siguiente sentido:

> El artículo 12, letra a), de la Directiva [95/46/CE] obliga a los Estados miembros a garantizar un derecho de acceso a la información sobre los destinatarios o categorías de destinatarios a quienes se comunican los datos y al contenido de la información comunicada, no sólo para el presente, sino también para el pasado. Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a ésta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la Directiva y, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento. (Asunto C-553/07 College van burgemeester y wehouders van Rotterdam v MEE Rijkeboer, 2007)

Acorde con lo anterior, y partiendo de la base en que se debe conservar la información, es menester aplicar técnicas de anonimización a los datos recopilados, de acuerdo con la legislación aplicable. En adición a lo anterior, el reglamento europeo, adolece de expresar el periodo de conservación de la información, por lo que proporciona cierta discrecionalidad a los Estados para que de forma autónoma lo determinen, y sea este el punto de partida entre la salvaguarda de los derechos fundamentales del titular de los datos y el interés del tratamiento de este.

b. No existe una técnica regulada para realizar tal procedimiento de anonimización, por lo que se deberá recurrir al estado del arte para tal efecto: en la actualidad, se han expedido numerosas guías que contemplan dos métodos para implementar el proceso de anonimización[11], la primera de ellas refiere al concepto de aleatorización, que se define como:

> […] una familia de técnicas que modifican la veracidad de los datos a fin de eliminar el estrecho vínculo existente entre los mismos y la persona. Si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta La aleatorización por sí sola no reduce la singularidad de cada uno de los registros, ya que estos pueden obtenerse a partir de un único interesado, pero sí puede proteger contra ataques o riesgos de inferencia. (Grupo De Trabajo Sobre Protección De Las Personas En Lo Que Respecta Al Tratamiento De Datos Personales, 2014, p.13)

Dentro de estas técnicas, se puede recurrir a procesos como la adición de ruido, la permutación y la privacidad diferencial, las cuales se procederán a describir de forma general a continuación, acorde con lo planteado por Grupo de Trabajo sobre Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, (2014):

- *Adición de ruido*: Consiste en modificar los atributos del conjunto de datos para que sean menos exactos, conservando no obstante su distribución general. Al tratar un conjunto de datos, cualquier observador supondrá que los valores son exactos, pero esto solo es cierto hasta cierto punto. Por ejemplo, aunque la altura de una persona se mida originalmente hasta el centímetro más próximo, el conjunto de datos anonimizado puede contener valores con una exactitud de ± 10 cm. Si se utiliza esta técnica de manera competente, un tercero

[11] Véase la "*guía orientaciones y procedimientos de anonimización expedida por la agencia española de protección de datos española"* o "*El Dictamen 05/2014 sobre técnicas de anonimización"* expedido por este mismo órgano.

no podrá identificar a una persona ni tampoco debería ser capaz de restaurar los datos o de averiguar cómo se han modificado.

- *Permutación:* Esta técnica consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados. Se trata de una estrategia útil en el caso de que sea importante conservar la distribución exacta de cada atributo en el conjunto de datos.
- *Privacidad diferencial:* pertenece a la familia de técnicas de aleatorización, aunque adopta un enfoque diferente. Mientras que, en la práctica, la inserción de ruido tiene lugar antes del momento en que se prevé difundir el conjunto de datos, la privacidad diferencial, por el contrario, puede usarse cuando el responsable del tratamiento de datos genera vistas anonimizadas de un conjunto de datos, al mismo tiempo que conserva una copia de los datos originales. Estas vistas anonimizadas normalmente se generan mediante un subconjunto de consultas de un determinado tercero. Este subconjunto contiene algo de ruido aleatorio que se añade de manera deliberada con posterioridad. La privacidad diferencial indica al responsable del tratamiento cuánto ruido debe añadir, y en qué forma, para obtener las garantías de privacidad necesarias. En este contexto, es especialmente importante una supervisión continua (como mínimo de cada nueva consulta) para evaluar cualquier posibilidad de identificación de una persona en el conjunto de resultados de las consultas. Sin embargo, conviene aclarar que las técnicas de privacidad diferencial no modifican los datos originales. Por lo tanto, según dicho estudio mientras se conserven los datos originales, el responsable del tratamiento es capaz de identificar a las personas a partir de los resultados de las consultas de privacidad diferencial mediante el conjunto de los medios que pueden ser razonablemente utilizados. Estos resultados también deben considerarse como datos personales.

Como se puede observar, las técnicas de aleatorización anteriores presentan una enorme dificultad, en términos de seguridad, esto habida cuenta que para agregar ruido sobre los datos objeto de protección se deberá conservar cierto grado de lógica respecto de los atributos que integran el conjunto de datos, lo que permitiría a una persona no autorizada identificar este tipo de falencias y hacer un filtro con el fin de conocer los datos reales.

De igual forma, para aplicar estas técnicas es necesario analizar los datos en conjunto, y de esta manera determinar cuáles son sujetos de anonimización mediante la aplicación de los procesos antes mencionados, por lo que las técnicas aleatorias suelen emplearse como una medida complementaria para la anonimización de los datos, por lo que suelen emplearse en combinación con procesos de generalización, la cual consiste en "generalizar o diluir los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes)". (Grupo de Trabajo sobre Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, 2014, p.17)

Dentro de estas técnicas, se puede recurrir a procesos como la agregación y anonimato, la diversidad y proximidad, así como la seudonimización, las cuales se procederán a describir de forma general a continuación[12]:

- *Agregación y anonimato k:* busca impedir que un interesado sea singularizado cuando se le agrupa junto con un número k de personas. Para lograrlo, los valores de los atributos se generalizan hasta el punto de que todas las personas acaban compartiendo el mismo valor.
- *Diversidad l, proximidad t:* extiende el anonimato k para garantizar que ya no se puedan realizar ataques por inferencia deterministas. Para ello, se asegura que, en cada clase de

[12] Tomado de Grupo De Trabajo Sobre Protección De Las Personas En Lo Que Respecta Al Tratamiento De Datos Personales, 2014, páginas 13 y ss.

equivalencia, todos los atributos tienen al menos l valores diferentes. Uno de los objetivos fundamentales consiste en limitar la ocurrencia de clases de equivalencia que tengan una variabilidad de atributos escasa. De esta forma, un atacante que posea conocimientos previos sobre un interesado en concreto siempre estará sometido a un grado significativo de incertidumbre.

Seudonimización: consiste en "la sustitución de un atributo (normalmente un atributo único) por otro en un registro, existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo." (Grupo De Trabajo Sobre Protección De Las Personas En Lo Que Respecta Al Tratamiento De Datos Personales, 2014, p.22)

Aplicando de forma correcta las técnicas antes mencionadas, se garantiza la seguridad de la información, que conllevaría la no recuperación concreta de datos puntuales que permiten individualizar a la persona, aunque esto no impide que se pueda realizar la plena identificación de la persona, por otros medios, como por ejemplo el uso de técnicas de ingeniería inversa ante la no adecuada aplicación de las técnicas generalizada y/o aleatorias. Adicionalmente, implementar la anonimización sin hacer un análisis de los riesgos inherentes a esta y en consideración al tipo de datos a tratar, puede acarrear la pérdida de control sobre los datos, ataques recurrentes y no integridad y disponibilidad de la información.

Encargado de la Protección de Datos

De acuerdo con la reglamentación europea en el artículo 28, el encargado del tratamiento de los datos será la persona que el responsable elija quien ofrecerá las garantías suficientes para aplicar las medidas técnicas y organizacionales apropiadas, que satisfagan los requerimientos legales y garantice la protección de los derechos de los titulares. La vinculación del encargado del

tratamiento se realizará a través de un contrato u otro acto jurídico, que conste por escrito, mediante el cual se especifique el objeto, la duración, la naturaleza, la finalidad del tratamiento y el tipo de datos y categorías de interesados, junto con las obligaciones y derechos del responsable. Sin embargo, por directriz del reglamento este contrato debe ser explícito en estipular que el encargado tratará los datos personales únicamente siguiendo las instrucciones documentadas del responsable, inclusive en la transferencia de los datos personales a un tercer país u organización (Reglamento General de la Protección de Datos, 2016).

En la práctica la aplicación del reglamento europeo está consagrada para todo tipo de entidades sean estas públicas o privadas, y todas ellas como responsables del tratamiento de los datos personales deberán designar un encargado del tratamiento, así la entidad se encuentre dentro o no de territorio europeo, cuando sus actividades involucren el tratamiento a gran escala de datos personales, tales como el origen étnico o racial, la opiniones políticas, las convienes religiosas o filosóficas, lo datos genéticos, biométricos, relativos a la salud u a la orientación sexual, entre otros.

Sin embargo, el reglamento europeo se limita a exigir la designación del encargado del tratamiento de los datos, pero no especifica el carácter o alcance que debe tener ese encargo; por lo cual serán las partes involucradas, el responsable y el encargado, quienes deben fijar sus derechos y obligaciones y los actos que puede realizar válidamente el encargado en nombre del responsable (López, 2018). De modo que la figura del encargo resulta ser una representación voluntaria directa, en la cual los actos del representante se transmitirán de forma automática a quien lo designó. Asimismo, sobre el encargado del tratamiento de los datos personales recae el deber legal de colaborar con las autoridades de control europeas, obligándolo a atender las consultas y requerimientos que directamente le dirijan (López, 2018).

En vista a que el GDPR, no especificaba el alcance de la relación jurídica entre el responsable y el encargado de la protección de datos, los Estados miembros de la Unión Europea se vieron en la necesidad de dar las directrices para estar en cumplimiento con la reglamentación. En el caso del gobierno español, las entidades que se encargan de la protección de datos en el territorio ibérico se unieron para emitir las directrices para la elaboración de los contratos entre el responsable y el encargado del tratamiento. En estas directrices, no solo se especifica de forma clara quienes pueden ser considerados como encargados del tratamiento, sino también los tipos de tratamiento (automatizado o no), el nivel de decisión del encargado, la forma de regulación de la relación entre el responsable y el encargado del tratamiento, el contenido mínimo del acuerdo o acto de encargo del tratamiento especificando; las instrucciones del responsable del tratamiento, el deber de confidencialidad, las medidas de seguridad que mitiguen los riesgos previstos por el responsable, el régimen de subcontratación (se presenta si el encargado del tratamiento requiere de otro encargado para desarrollar el servicio encomendado), el manejo de los derechos de los interesados, las obligaciones del encargado para garantizar el cumplimiento de las medidas de seguridad y el destino de los datos al finalizar la prestación del servicio. Además, estas directrices traen como anexo un formato del tipo de acuerdo que se puede realizar entre el responsable y el encargado.

Debido a que la figura del encargado de la protección de datos estaba establecido desde la directiva 95/46 de la Comunidad Europea, con el reglamento del 2016 no se generó un cambio radical para para el cumplimiento del mismo, pero permitió que los Estados miembros se vieran en la necesidad de buscar regulaciones específicas y locales que les permitieran dar cumplimiento a la regulación de la protección de datos y así garantizar el derecho de habeas data de todos aquellos ciudadanos que habitan en la Unión Europea.

En Colombia, es importante resaltar que la Ley Estatutaria 1581 de 2012 define al encargado del tratamiento como la persona natural o jurídica, que por sí misma o en asocio con otros, realiza el tratamiento de los datos personales, quien junto con el responsable tiene el deber de garantizar el principio de transparencia y seguridad con los titulares de los datos. Esta, al igual que en la reglamentación europea, debe ser aquel que protege los derechos de los titulares y es el punto de contacto para efectos de consulta y reclamos. El título VI de la ley de habeas data, recopila los deberes que debe cumplir el encargado del tratamiento, no solo con los titulares, sino con respecto a la Superintendencia de Industria y Comercio como ente de supervisión y control. Cabe resaltar que, a diferencia con la regulación europea, la legislación colombiana no hace referencia alguna en la forma mediante la cual se debe regular la relación entre el responsable y el encargado del tratamiento.

Empero, la Corte Constitucional en su control constitucional fue expresa en determinar que el encargado del tratamiento no puede ser el mismo responsable, por lo cual deben existir dos personas independientes e identificables, en donde el responsable le señala al encargado cómo se requiere el procesamiento de los datos, es decir, el encargado recibe las instrucciones sobre cómo los datos serán administrados, haciendo implícita de esta forma la subordinación que tiene el encargado del tratamiento frente al responsable (Sentencia C-748/11, 2011).

El Decreto 1074 de 2015, que reglamentó parcialmente la ley estatutaria de habeas data, si bien es cierto diferencia al responsable y al encargado del tratamiento de los datos, les otorga una similitud jerárquica que es casi indiscernible, y en ningún momento, como ocurre dentro de la jurisdicción europea, hay una directriz que informe o promueva el diseño de un contrato en el cual se estipulen de forma clara y expresa las funciones que los encargados deben desarrollar.

Por lo anterior, todas aquellas entidades, empresas, propiedades horizontales, negocios entre otros, que dentro de su normal actuar reciben y operan datos personales, pueden estar vulnerando los derechos de los titulares, puesto que, aunque la Ley regula el deber ser de los encargados del tratamiento, la norma reglamentaria no enfoca su texto en cuáles son las condiciones que debe cumplir el encargado y su real diferencia con el responsable de datos. En la práctica, esta falta de distinción es de fácil percepción, hoy en día no es común encontrar en los diferentes puntos de contacto de las organizaciones que operan datos personales la identificación de quien es el encargado del tratamiento de datos y quien es el responsable. Bajo el mismo derrotero, la Superintendencia Financiera[13], ha expedido diferentes resoluciones donde se reiteran los deberes y funciones del encargado y el responsable del tratamiento de datos, sin que exista una diferenciación clara respecto al alcance del primero y el segundo, así como las responsabilidades que ostentan, lo cual va en contravía de lo que ha expresado la Corte Constitucional respecto a la diferencia de estos.

Registro de las actividades del Tratamiento de Datos

Teniendo en cuenta la importancia de la protección del derecho de habeas data, por el cual es necesario llevar un registro de las actividades adelantadas por el responsable y encargado del tratamiento de datos en el cual se pueda hacer seguimiento de la forma en la cual los datos personales han sido manejados, el GDPR de la Unión Europea ha establecido unos criterios mínimos de información que este registro de actividades debe contener para mitigar los riesgos

[13] Resolución 75761 de 2021, Resolución 74238 de 2021, Resolución 71102 de 2021, Resolución 69443 de 2021, Resolución 64454 de 2021.

que se puedan presentar con el manejo de los datos personales y evitar posibles vulneraciones a los derechos y libertades de los titulares de los datos.

Por este motivo, a través de artículo 30 del reglamento se regula la información que debe contener el registro de las actividades del tratamiento efectuadas bajo la responsabilidad del responsable del tratamiento de los datos. Asimismo, regula la información que debe contener el registro de actividades del encargado del tratamiento de datos. Es menester aclarar que tanto la jurisdicción europea como la colombiana, contemplan que el responsable y el encargado del tratamiento de datos son dos funcionarios independientes, por lo cual su registro de actividades, por extensión, también deberá ser independiente.

Para el caso del responsable del tratamiento de datos, la regulación europea expresa que el registro de actividades debe contener su nombre y datos de contacto, los fines para los cuales ha sido recaudados los datos que están a su disposición, una descripción tanto de la categoría de usuarios de quienes su entidad posee la información, como de la categoría de los datos personales que almacena. Si la entidad realiza transferencia internacional de datos, es necesario informar la clase de destinatarios a quienes se les comunicaron los datos personales, así como la identificación del tercer país u organización internacional, junto con la documentación que respalde las garantías adecuadas que tiene el destinatario internacional para la protección de los datos personales de titulares europeos. Si es posible, es necesario informar los plazos previstos para la supresión de datos, según las categorías de datos que la entidad recoge y finalmente, pero no menos importante, la descripción general de las medidas técnicas y organizativas implementadas por la entidad responsable del tratamiento de datos, que demuestren la protección en la seguridad de los datos personales recibidos. (Artículo 30 del General Data Protection Regulation GDPR)

En el caso del registro de actividades que debe realizar el encargado del tratamiento de datos, la información a consignar es semejante a la solicitada el responsable del tratamiento, con la diferencia que el encargo del tratamiento debe incorporar el registro de los tratamientos efectuados por cuenta del responsable, puesto que el encargado del tratamiento de datos trabaja para el responsable bajos los criterios establecidos por el contrato y deberá informar cuales fueron las actividades que se desarrollaron en el tratamiento de datos, en relación con lo especificado en dicho contrato.

La realización de este registro se enmarca en el deber de transparencia y control de seguridad que se les exige a las entidades que por su actividad deben recolectar datos personales de los ciudadanos europeos. Este registro debe ser presentado a las autoridades de control establecidas por cada Estado y se deberá presentar de forma escrita, aunque, la regulación exceptúa de este registro de actividades a las empresas que cuentan con menos de 250 empleados, a menos que su actividad pueda entrañar algún riesgo para los derechos y libertades de los titulares de los datos o que por sus actividades deban recolectar categoría de datos especiales, acorde con el artículo 30, numeral 5 del mismo reglamento.

De acuerdo con la Agencia Española de Protección de Datos[14], le corresponde a cada organización , según el principio de responsabilidad proactiva (Accountability), determinar el nivel de segregación o de inclusión de información con el que desea registrar el tratamiento de datos que requiera su actividad, asimismo, le corresponde ponderar la gestión de la utilización de datos dentro de su organización, para que esta resulte útil, ágil, efectiva y le permita el

[14] La Agencia Española de Protección de Datos es la autoridad independiente encargada de velar por la privacidad y la protección de datos de la ciudadanía española. Busca fomentar que las personas conozcan sus derechos ofrece posibilidades para que los ciudadanos puedan ejercerlos. Asimismo, ayuda a los sujetos obligados para que tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa.

cumplimento de la finalidad de la regulación europea, es decir, el control efectivo de los datos personales por parte de los titulares, para proteger sus derechos y libertades (Agencia Española Protección de Datos, 2018)

La legislación en Colombia a través no solo de la Ley estatutaria, sino mediante el Decreto 1074 de 2015, reglamenta la responsabilidad demostrada frente al tratamiento de datos personales por parte del responsable y el delegado de la protección de datos personales, a quienes de forma explícita les solicita que en su capacidad de ejercicio deben tener la posibilidad de demostrar ante la Superintendencia de Industria y Comercio que se han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones de la Ley 1581 de 2012, y en este sentido deberán proporcionar, cuando se le requiera, la siguiente información; naturaleza jurídica del responsable y su tamaño empresarial, naturaleza de los datos personales, objeto del tratamiento, el tipo de tratamiento y la evaluación de los riesgos potenciales que el referido tratamiento puede causar a los derechos del titular de los datos. (Decreto 1074 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo - Sección 6 del capítulo 25 de la parte 2, 2015)

Igualmente, complementa la responsabilidad demostrada con normas corporativas vinculantes, que han de ser desarrolladas por cada entidad que realiza tratamiento de datos personales, las cuales deben ser presentadas ante la Superintendencia para su aprobación. Si bien en comparación con la regulación europea, este no es un registro en donde es necesario informar las actividades, sí debe informar sobre las medidas técnicas y organizativas que se implementan para cumplir con las obligaciones de la norma estatuaria para la protección de habeas data.

En similar sentido, la regulación en Colombia desarrolló a través de la norma de habeas data el Registro Nacional de Bases Datos, este registro busca; i). que todos los ciudadanos

conozcan cuales son las bases de datos que funcionan en el país y ii). que la Superintendencia tenga un control preciso sobre estas bases para que pueda establecer quien, y como se trata la información personal de los colombianos en el país y de ser necesario, ejercer sus potestades sancionatorias, si percibe que quienes son responsables o encargados del tratamiento de datos están incurriendo en la inobservancia de la Ley.

> *"[…] el objetivo de la centralización de esta clase de información por parte de un órgano del Estado es facilitar el ejercicio de uno de los ámbitos esenciales del habeas data: conocer quién está haciendo tratamiento de datos personales, a fin de que pueda existir un control efectivo de éstos por su titular, hecho que explica por qué dicho registro es abierto a la consulta del público en general. En ese orden ideas, la inscripción en él se debe imponer como una obligación tanto para las bases públicas como privadas, pues este es un instrumento que permitirá que el Estado efectivamente garantice que el titular del dato pueda tener un control efectivo sobre sus datos personales[.]" (*Sentencia C-748/11, 2011)

En cumplimiento del objetivo argumentado por la Corte Constitucional, el Decreto 1074 de 2015 especifica qué información mínima debe contener el registro y detalla los términos y condiciones que se deben surtir para la inscripción al registro por parte de las organizaciones que recolectan datos personales en el país. La información mínima del registro, acorde al artículo 2.2.2.26.2.1 del mencionado decreto, será la identificación, ubicación y contacto del responsable y el encargado del tratamiento, lo canales que se implementaron para que el titular ejerza sus derechos, nombre y finalidad de la base de datos, forma del tratamiento de la base de datos (manual o automatizada) y la política del tratamiento de la información. Sobre los términos y condiciones, la inscripción al Registro Nacional de Bases de Datos, tuvo un plazo especifico dependiendo de

las los activos reportados por las organizaciones para realizar su inscripción o si su naturaleza jurídica era pública, so pena de sanciones por no realizar el registro y reguló las posteriores actualizaciones al registro, las cuales deben realizarse dentro de los 10 primeros días hábiles del mes cuando existan cambio sustanciales o anualmente durante el primer trimestre del año a partir del 2020.

Como se puede notar, ambas legislaciones regulan la forma en la cual los responsables y los encargados de la protección de datos deben registrar sus actividades en el manejo de los datos personales. El fin último de estos registros es incentivar la responsabilidad demostrada (accountability) para proteger los derechos y libertades de los ciudadanos de cada jurisdicción. En la medida que ambas jurisdicciones contemplan la diferencia entre el responsable y el encargado de la protección de datos, existe una mayor transparencia si el registro se realiza de forma independiente, como ocurren en la legislación europea. Sin embargo, para ejercer un mejor ejercicio del derecho de habeas data, que el registro sea público, como ocurre en la legislación colombiana, le permite al titular un mayor acceso a la información sobre el tratamiento de sus datos, no solo por parte del responsable y/o encargado sino también por parte de la entidad reguladora, en este caso la Superintendencia de Industria y Comercio.

CAPÍTULO V. AUTORIDAD DE PROTECCIÓN DE DATOS Y SANCIONES

Las jurisdicciones bajo análisis prevén en sus respectivas regulaciones la creación de una entidad independiente que se encargue de la supervisión y ejecución de lo prescito en el Reglamento Europeo y en la Ley 1581 de 2012 respectivamente. Principalmente, lo que se busca

es la protección efectiva del derecho de habeas data de los ciudadanos, así como la garantía de sus derechos y libertades.

Autoridad De Protección De Datos

Desde la perspectiva europea y el lineamiento con su Reglamento, esta autoridad de control deberá ser establecida por cada Estado miembro, que se encargará de la aplicación coherente del GDPR. Estas entidades deberán ser creadas de acuerdo con la normatividad interna de cada Estado y se deberá informar su creación a la Comisión Europea para la Protección de Datos.

Las autoridades estatales de protección de datos tendrán completa independencia para el desempeño de sus funciones y el ejercicio de sus poderes, al igual que sus miembros. El Estado miembro debe asegurar para estas entidades de control la disposición de recursos humanos, técnicos y financieros para el efectivo cumplimento de sus funciones. Las competencias de estas entidades serán establecidas por el gobierno local, pero deberán contener de forma necesaria las competencias que el reglamento establece tales como; actuar como autoridad de control principal, recepción de reclamaciones por posibles infracciones al reglamento y ser único interlocutor para el tratamiento transfronterizo de datos realizado por los responsables o encargados del tratamiento de datos.

El mismo Reglamento establece de forma general las funciones que esta entidad de control deberá ejercer en el Estado miembro, sin limitación a adicionar otras funciones según las necesidades previstas por el gobierno central. Principalmente deberá controlar la aplicación del Reglamento, será el responsable de promover la compresión al público de la norma, los riesgos, normas, garantías y derechos en relación al tratamiento, deberán asesorar las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas, tratar

las reclamaciones presentadas por un interesado, organismo, organización o asociación e investigar de forma oportuna el motivo de dicha reclamación, hacer seguimiento de los cambios que sean de interés y que tengan incidencia en la protección de datos, ofrecer asesoramiento sobre las operaciones de tratamiento de datos, llevar registros internos de las infracciones al reglamento, entre otras.

De igual manera, el Reglamento le otorga poderes especiales a las autoridades de control de los Estados miembros, que les permiten investigar y controlar el tratamiento de datos en sus respectivos países. Por lo anterior, la autoridad de protección de datos podrá ordenarle al responsable o encargado del tratamiento que facilite información sobre el desempeño de sus funciones, llevar a cabo auditorias sobre protección de datos, notificar al responsable o encargado del tratamiento presuntas infracciones al reglamento, emitir advertencias y/o ajustes, limitar temporal o definitivamente de las actividades de los responsables y encargados de protección de datos, imponer multas administrativas, emitir por iniciativa propia o previa solicitud dictamen direccionados al gobierno local, y otros poderes especiales descritos en el artículo 58 del Reglamento.

De acuerdo con la Comisión Europea para la Protección de Datos, existen registradas 30 autoridades de control, incluyendo aquellas de los países que hacen parte del EFTA[15] (Islandia, Liechtenstein y Noruega). La Comisión en sí misma es una autoridad independiente que contribuye, junto con las autoridades de cada Estado miembro, a la aplicación continua de las reglas de protección de datos y promueve la cooperación entre las autoridades de protección de datos europeas. La ruta de trabajo para el 2021/2022 está fundamentada en cuatro pilares principales, el

[15] European Free Trade Association

primero busca avanzar en la armonización y la facilidad del cumplimento, a través de la promoción de herramientas que promuevan la puesta en práctica de la protección de datos, teniendo en cuenta la experiencia de los países miembros. El segundo pilar busca apoyar de forma efectiva la cooperación entre las autoridades de supervisión nacionales, mediante la dinamización de los procesos internos, combinado las experiencias y promoviendo una mejor coordinación entre las autoridades. El tercer pilar buscar acercar la garantía de los derechos fundamentales a las nuevas tecnologías, el objetivo es supervisar las tecnologías nuevas y emergentes y su potencial impacto en los derechos fundamentales de los individuos, para mantener no solo las reglas en constante actualidad sino proteger a los ciudadanos europeos, y finalmente el cuarto pilar busca una dimensión global, para promover estándares globales para la transferencia de datos internacionales y reforzar la promoción del modelo de protección de datos europeo a nivel global. (European Data Protection Board, 2021, pp 2-5)

Dentro de las autoridades locales una de las más activas es la Agencia Española de Protección de Datos; esta es una autoridad administrativa independiente, prevista en la Ley 40 de 2015 de la jurisdicción española. Constituye la autoridad de control del GDPR. La agencia protege los derechos de acceso, rectificación, limitación, oposición, supresión, portabilidad de los ciudadanos españoles. Asimismo, ha emitido diferentes guías para garantizar el derecho de habeas data y para la promoción y sensibilización de los diferentes ámbitos aplicables a la protección de datos.

En la jurisdicción colombiana la autoridad de protección de datos fue establecida directamente en la Ley 1581 de 2012, a través del artículo 19, el cual determina que la entidad pública encargada de la vigilancia para garantizar que en el tratamiento de datos se respeten los principios, derechos, garantías y procedimientos es la Superintendencia de Industria y Comercio, por medio de la

Delegatura para la Protección de Datos Personales. Al respecto la Corte Constitucional, en la sentencia C-748 (2011) expresó que la protección de datos no solo requiere de una regulación que consagre los principios, derechos, deberes y responsabilidades que rigen el tratamiento del dato, sino también de una institucionalidad que permita un control y ámbito de garantía efectiva del derecho de habeas data. Como derecho autónomo, requiere de mecanismos efectivos de protección que solo no debe depender de los jueces, sino también de una institucionalidad administrativa que asegure la observancia efectiva de la protección de datos y debido a su carácter técnico, tenga la capacidad de fijar política pública en la materia.

Las funciones a desarrollar por la Delegatura de Protección de Datos de la Superintendencia están, asimismo, enmarcadas en la ley estatutaria, principalmente debe velar por el cumplimiento de legislación; sobre este aspecto la Superintendencia en el último quinquenio ha realizado publicaciones, capacitaciones, foros, congresos, eventos, visitas administrativas y ha promulgado ordenes, sanciones, formulaciones de cargos y atención a quejas. Dentro de sus publicaciones más recientes se encuentra la Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales, la Guía de Tratamiento de las Fotos como datos Personales y la Guía sobre el Tratamiento de Datos Personales en la Propiedad Horizontal. De igual manera tiene la potestad de iniciar investigación de oficio o a petición de parte por vulneraciones al derecho de habeas data y a través de estas ordenar las medidas necesarias para garantizar este derecho fundamental. Puede además disponer del bloqueo temporal de datos, para abril del 2021 la Superintendencia había realizado 12 solicitudes desde el año 2018. Al igual que en la regulación europea, la autoridad en Colombia debe promover y divulgar los derechos de las personas con el tratamiento de datos personales, por lo cual la Delegatura ha realizado concursos educativos fomentando la pedagogía con los jóvenes bachilleres y de educación superior, y ha implementado

varias campañas de divulgación a nivel nacional. (D. P. la P. de D.-S. de Industria y Comercio, carta, abril 20 de 2021)

La Superintendencia también debe impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables y encargados de la protección de datos, esta actividad principalmente está ejecutada a través de las órdenes que la Dirección de Investigaciones de Protección de Datos Personales emite promoviendo el mejoramiento de los procesos, procedimientos y políticas. En la jurisdicción colombiana, la autoridad de protección de datos debe administrar el Registro Nacional Público de Bases de Datos, para este fin la Superintendencia para el año 2018 profirió el Decreto 090 del 19 de enero de 2018, la Circular Externa 03 del 1 de agosto de 2018 y la Circular Externa 01 del 16 de enero de 2019, las cuales establecen y depuran las obligaciones del registro de bases de datos.

Por otro lado la Superintendencia también como autoridad de control ha establecido relaciones con otras autoridades de protección de datos en Latinoamérica y Europa, razón por la cual, hoy día, hace parte de la Red Iberoamericana de Protección de Datos, organización que desarrolla iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica y promueve los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales. A esta red pertenecen 12 autoridades de protección de datos y para el periodo de 2021-2022 la presidencia de la red está en cabeza del delegado de Protección de Datos de las Superintendencia de Industria y Comercio de Colombia.

Cabe destacar las autoridades de control en la jurisdicción europea y colombiana son similares, puesto que las funciones impuestas por las regulaciones son similares y las autoridades cumplen con la misión de promover la protección del derecho de habeas data. Sin embargo, pese a los esfuerzos hechos por la autoridad en Colombia, es necesario mejorar la supervisión que se

realiza a los responsables y encargados del tratamiento, en la medida que no existe un total alcance del Registro Nacional de Base de Datos y esta misma herramienta no informa de forma efectiva el mecanismo que los responsables y encargados del tratamiento de datos establecieron para la protección del derecho de habeas data. Asimismo, en la práctica es palpable una falencia en la información suministrada a los titulares de los datos, sobre sus garantías y derechos, puesto que se requiere de una campaña masiva en los diferentes grupos sociales.

Sanciones

El capítulo VIII del GDPR en la jurisdicción europea prevé los recursos, responsabilidad y sanciones que pueden ser aplicables ante la vulneración de los derechos y libertades de los titulares de los datos personales por parte de los responsables y encargados del tratamiento. El reglamento establece que todo interesado puede presentar una reclamación ante la autoridad de control, si considera que el tratamiento de datos personales que le contiene infringe el reglamento, y de igual manera podrá el interesado ejercer la tutela judicial efectiva cuando considere que se ha vulnerado los derechos fundamentales de habeas data. En razón a la tutela judicial, el reglamento prevé responsabilidad civil e indemnización por daños y perjuicios materiales o inmateriales que haya sufrido el interesado como consecuencia de la infracción al Reglamento por parte del encargado o el responsable del tratamiento. (Regulación General de protección de Datos, 2016)

Asimismo, la autoridad de protección de datos puede, como ente de control, imponer multas administrativas por las infracciones al reglamento, estas multas dependiendo de las circunstancias concretas pueden ser a título adicional o sustitutivo de las medidas de advertencia contemplada por la misma autoridad. Para determinar el quantum de la multa es necesario evaluar la intencionalidad, las medidas de reparación por parte del responsable o del encargado, las

medidas de cooperación adoptadas para finiquitar la infracción y la mitigación de riesgos, las categorías de datos personales afectados por la infracción, la forma en que tuvo conocimiento de la infracción la autoridad de control y cualquier otra circunstancia agravante o atenuante aplicable al caso concreto, según lo establecido en el artículo 83. La multa será de 10 millones de euros, o si es una empresa, del 2% del volumen del negocio total anual global si la infracción es relacionada con las obligaciones del encargado y del responsable del tratamiento, de los organismos de certificación y del organismo de supervisión. La multa será de 20 millones de euros ,o si es una empresa, del 4% del volumen de negocio total anual global si la infracción está relacionada con los principios básicos del tratamiento y las condiciones del consentimiento, los derechos de los interesados, las transferencia indebidas de datos a destinatarios internacionales, por sentencia judicial emitida por los Estados miembros y por el incumplimiento de una resolución o una limitación temporal o definitiva del tratamiento emitida por la autoridad de control.

La última decisión vinculante en relación con las multas administrativas tomada por el Comité Europeo de Protección de Datos es relativa a un conflicto planteado por otras autoridades de control interesadas, en relación con la decisión tomada por la autoridad de control irlandés en contra de WhatsApp Ireland Limited, el cual se inició de oficio en diciembre de 2018 con el objetivo de determinar si la empresa cumplía con las obligaciones del Reglamento General de Protección de Datos. De acuerdo con la otras autoridades de control interesadas, esta decisión no contemplaba medidas sobre el proceso especifico de anonimización, las posiciones de compromiso no eran aceptables dado la gravedad de las infracciones cometidas por WhatsApp Ireland Limited y la sanción no era disuasiva, proporcionada y disuasoria, puesto que si bien se aplicó lo relativo al quantum que establece el reglamento en relación al porcentaje del volumen del negocio anual global, no se tuvo en cuenta la “unidad económica única”, y por lo tanto el cálculo de la multa

puede diferir, acorde con el artículo 65 del reglamento. Una unidad económica única se conforma por varias empresas en las cuales hay una entidad controlante y varias subsidiarias, en este caso la entidad controlante es Facebook Inc., por lo cual para determinar el volumen del negocio total es necesario saber el volumen del negocio de cada una de las empresas que conforman la unidad económica. De igual manera, la multa administrativa será el resultado del análisis de todas las infracciones cometidas según su gravedad, no se determinará por la individualidad de la infracción, su aplicación debe ser efectiva, proporcionada y disuasoria dentro del límite de la infracción más grave. En razón a lo anterior, las autoridades de control interesadas determinaron que la multa impuesta por la autoridad de control en Irlanda no era suficiente en relación con las infracciones cometidas por WhatsApp Ireland Limited y su cálculo no estaba contemplando la unidad única económica, lo cual afecta el carácter intencionado de la infracción. Después del análisis del Comité Europeo, se determinó la reevaluación de la multa administrativa. (*Decisión vinculante 1/2021 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con WhatsApp Ireland con arreglo al artículo 65, apartado 1, letra a), del RGPD*, s/f)

Ahora en bien, en la legislación colombiana las sanciones están establecidas en la Ley estatutaria en el capítulo II del Título VII, según el cual la Superintendencia es quien impone las sanciones por el incumplimiento de la Ley por parte de responsable o el encargado del tratamiento de los datos. Dentro de las sanciones establecidas en la regulación se encuentra las multas de carácter personal o institucional hasta por dos mil salarios mínimos mensuales vigentes al momento de su imposición, estas multas pueden ser sucesivas mientas subsista el incumplimiento. Para el año 2022, la multa estaría estipulada en 2 mil millones de pesos (cerca de 477 mil euros). Otro tipo de sanción es suspensión de actividades relacionadas con el tratamiento por un término de seis meses, el cierre temporal de las operaciones relacionadas con el tratamiento, si no son

adoptados lo correctivos necesarios requerido en la suspensión y finalmente el cierre inmediato y definitivo de la operación que involucre el tratamiento de datos, acorde con el artículo 23 de la Ley 1581 de 2012. Sobre este particular, es importante resaltar que, en comparación con la regulación europea, en Colombia la sanción más grave es el cierre de actividades, mientras que en la jurisdicción europea es la imposición de una multa administrativa con un límite porcentual del volumen del negocio total.

En relación con los criterios para evaluar las sanciones imponer, ambas jurisdicciones las expresan en sus regulaciones, en Colombia esos criterios son la dimensión del daño o peligro a los intereses jurídicos tutelados, el beneficio económico que obtuvo el infractor, la reincidencia en la infracción, la conducta del infractor en contra de la acción investigativa por parte de la Superintendencia. La renuencia o desacato para cumplir las órdenes impartidas y por último la aceptación expresa de la infracción por parte del investigado previo a la imposición de la sanción. (artículos 83 del GDPR y Articulo 23 de la Ley 1581 de 2012)

De acuerdo con la Delegatura para la Protección de Datos de la Superintendencia, a través de la Dirección de Investigaciones de Protección de Datos Personales desde el 2018 hasta el primer trimestre del 2021 se habían impuesto un total de 217 sanciones, de las cuales 79 corresponden a sanciones en relación con la Ley 1581 de 2012, como lo muestra la tabla 2, la cual fue suministrada acorde al derecho de petición elevado mediante número de radicado 21-104275-4 de fecha abril 20 de 2021, obteniendo lo siguiente:

Tabla 2

Sanciones impuestas por la delegatura de protección de datos de la SIC

LEY 1581					
Mes/año	2018	2019	2020	2021	
Enero	1	0	1	0	
Febrero	7	0	0	1	
Marzo	0	0	0	3	
Abril	4	3	0	2	
Mayo	1	9	0		
Junio	2	3	0		
Julio	0	1	1		
Agosto	2	2	1		
Septiembre	1	1	7		
Octubre	1	1	9		
Noviembre	1	1	4		
Diciembre	5	0	4		
TOTALES	25	21	27	6	79

Nota: Esta tabla ilustra el número de sanciones impuestas por mes desde al año 2018 a 2021, ante incumplimientos a la normativa de protección y tratamiento de datos

Conforme al principio de proporcionalidad que orienta el derecho administrativo sancionatorio, la sanción a imponer debe ser equilibrada en relación con su monto y la finalidad que la norma vulnerada establezca, la proporcionalidad implica que la sanción administrativa no resulte excesiva en rigidez, ni carente de importancia frente a esa misma gravedad. (Resolución 17360 de 2022, 2022)

Cabe resaltar que para determinar el monto de sanción la Dirección de Investigaciones evalúa los estados financieros y tamaño de la empresa, sin embargo, no es una información determinante puesto que lo importante es el grado de afectación al derecho fundamental vulnerado y la sanción deberá ser por tal motivo disuasorio y no confiscatoria, misma premisa es implementada por la jurisdicción y la autoridad de datos en Europa.

CONCLUSIONES

Los datos personales son hoy en día una información de suma importancia para los ciudadanos de un Estado, puesto que del efectivo tratamiento se está protegiendo un derecho fundamental y de la correcta regulación estatal sobre este aspecto, se garantiza la privacidad de esta información tan sensible para cada individuo. Es innegable que el avance tecnológico, pero en especial la pandémica causada por el SARS-COVID 19, llevó a la digitalización de muchos servicios, en los cuales los individuos otorgaban sus datos personales a diferentes entidades, ignorando los derechos que les amparan y las responsabilidades que estas entidades deben tener con sus datos.

Si bien es cierto, las regulaciones analizadas en esta monografía datan del 2012 en Colombia y 2016 en Europa, su aplicabilidad tomó mayor relevancia en tiempos de pandemia y post- pandemia, puesto que la digitalización es un proceso que llegó para quedarse y avanzar a otras tecnologías que en un futuro no solo utilizarán los datos que hoy en día se protegen, sino también datos aún más privados o sensibles, los cuales siempre requerirán un mejor y más fortalecida regulación.

Después de un acucioso análisis comparativo realizado a la Ley 1581 de 2012, al Decreto 1074 de 2015, por el cual parcialmente se reglamentó la Ley mencionada y el Reglamento General de Protección de Datos de la Unión Europea, es posible determinar que en la jurisdicción colombiana desde la perspectiva constitucional para la protección y garantía del derecho de habeas data, la Ley 1581 de 2012 y su Decreto reglamentario, protegen y otorgan los derechos de acceso, rectificación, supresión y oposición a los titulares de los datos personales y responden de forma

asertiva a las necesidades respecto de la forma en que los responsables y/o encargados realizan la recolección, tratamiento y procesamiento de los datos.

Sin embargo, la Ley en Colombia debe implementar mejoras para que la garantía del derecho de habeas data sea más efectivo en la materialización del mismo y es en este ámbito fue donde se encontró las mayores diferencias entre las jurisdicciones.

Respecto de los principios, el marco legal colombiano aborda 8 postulados, a diferencia de la UE, que encuentra su sustento en solo 6; es necesario mencionar que Colombia considera el principio de acceso y circulación restringida como bases de su sistema legal, en lo que se refiere al tratamiento de datos personales. A contrario sensu, la regulación europea sustenta la garantía del derecho de habeas data en el principio de transparencia, el cual a su vez es reconocido como un derecho de los titulares de los datos, lo que implica que deben cumplirse de la forma en la que se establece en el GDPR. Para este cumplimiento el consentimiento es de suma importancia y debe ser entregado para cualquier tipo de tratamiento (comercial, laboral, legal, etc.), el cual de forma explícita en el RGDP debe ser de fácil acceso y entendimiento y evitar cualquier tipo de ambigüedad, el titular deber ser completamente informado sobre sus derechos, finalidad del tratamiento de datos, tiempo del tratamiento y su revocación puede darse en cualquier momento. Si bien en Colombia para el tratamiento de los datos se requiere de un consentimiento previo, similar en contenido al consentimiento europeo, el titular no tiene la potestad de revocarlo y solo podrá realizarse a través de la Superintendencia de Industria y Comercio, limitando el libre derecho de supresión del titular de datos al ciudadano titular de los mismos.

La norma europea dentro del derecho de supresión otorgado a los ciudadanos establece el derecho al olvido digital, que le garantiza al ciudadano europeo, la supresión total de sus datos en el ámbito virtual, como de su huella digital evitando posibles daños en el futuro de la libertad o

dignidad del titular, puesto que los datos personales no serán tratados a perpetuidad por el responsable de los mimos. Lamentablemente en Colombia, el derecho al olvido digital no ha podido ser implementado a cabalidad, puesto que se ha manifestado dentro de las discusiones del Congreso, la posibilidad que su aplicación puede generar censura de información necesaria, en relación con la investigación judicial para los servidores públicos, poniendo en riesgo los derechos y libertades de los ciudadanos, lo que deja sin herramientas a los ciudadanos, en caso tal de que los mismos, como titulares de los datos deseen retirarlos de la red, puesto que no son necesarios para el fin que fueron obtenidos, o los mismos se encuentran en la internet sin el consentimiento del titular, afectando derechos como el honra, buen nombre, entre otros.

Dentro del sistema europeo el tratamiento de los datos personales es analizado desde la perspectiva del riesgo, por lo que se impone la obligación a los responsables de adoptar la implementación de la protección desde el diseño y por defecto, como una medida proactiva (accountability) que evite la materialización de riesgos inherentes al tratamiento y procesamiento de datos recolectados por plataformas y/o herramientas informáticas, lo que implica, un cambio cultural en lo que tiene que ver con la manera en la que las organizaciones diseñan las políticas de control y mitigación del riesgo. En Colombia, por el contrario, hoy en día el desarrollo de esta figura se ha efectuado por medio de guías expedidas por parte de la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, documentos que carecen de carácter vinculante, por lo que son abordadas por las organizaciones como meras recomendaciones sujetas a su adopción de forma discrecional por parte de estas. Por lo tanto, en Colombia es necesario reglamentar las medidas proactivas para la mitigación de riesgos en el tratamiento de datos personales, fortaleciendo la garantías y derechos del titular de los datos y mejorando la protección desde el responsable y encargado del tratamiento de datos.

Adicionalmente en el derecho colombiano es necesario mejorar la diferenciación que hay entre el encargado y el responsable de datos, si bien la Ley consagra a los dos cargos como individuos independientes, en la práctica las entidades que hacen el tratamiento de datos no diferencian estas dos responsabilidades, evitando que la Ley sea aplicada a cabalidad. Es tal el desconocimiento que existe sobre las diferentes funciones del responsable y el encargado de datos, que, durante el 2022 de las 13 sanciones impuestas por la Dirección de Investigación de Protección de Datos Personales, 11 sean sobre las funciones que deben cumplir los responsables y encargados de datos, sin mencionar las sanciones de años anteriores. Adicionalmente, es imperativo que se reglamente por parte de autoridad de control, la relación jurídica que se puede establecer entre el responsable y el encargado de datos, para diferenciar funciones y responsabilidades ejerciendo el principio de transparencia, seguridad y confidencialidad establecidas en la Ley.

La Superintendencia de Industria y Comercio como autoridad de control ha hecho un buen desarrollo doctrinal para el tratamiento de datos personales a través de la Delegatura de Protección de Datos Personales, sin embrago, es necesario mejorar la interacción con los ciudadanos en todos los rangos de edad, para mejorar los mecanismos de información sobre derechos y procedimientos establecidos para la protección de datos personales. Adicionalmente es oportuno mejorar la supervisión que se realiza a los responsables y encargados del tratamiento, en la medida que no existe un total alcance del Registro Nacional de Base de Datos y esta misma herramienta no informa de manera efectiva el mecanismo que los responsable y encargados del tratamiento de datos establecieron para la protección del derecho de habeas data.

En cuanto a las sanciones, el régimen europeo impone multas con mayor severidad a las empresas que no den estricto cumplimiento a la protección de datos personales de los ciudadanos que hacen parte de la Unión Europea, por lo cual la mayoría de las organizaciones que recolectan

información de los ciudadanos que integran este bloque común han venido efectuando diferentes políticas y planes con el ánimo de responder a las exigencias de la nueva normativa, lo que contrasta con las sanciones impuestas por la Superintendencia colombiana ante el incumplimiento de los postulados de la Ley 1581 de 2012, que al ser vistas desde de una perspectiva económica, resultan ser medidas un tanto ineficientes en atención a que en ocasiones muchas de las sanciones son por incumplimiento reiterado al marco legal a compañías ya sancionadas, así como el adolecer de medidas tendientes a la protección de los datos personales que son obtenidos por empresas mediante la red, por lo que, en muchas ocasiones, el inadecuado tratamiento de los datos personales por parte de estas, no es objeto de investigación y/o sanción por parte de la Superintendencia de Industria y Comercio, al escapar del factor territorialidad de la norma.

En resumen, la Ley 1581 del 2012 es una garantía del Estado Colombiano a la protección del derecho fundamental de habeas data, sin embargo es necesario mejorar y actualizar el Decreto reglamentario de la Ley estatutaria, para adicionar temas necesarios como la responsabilidad proactiva, el derecho al olvido y su aplicabilidad en conexión con otros derechos como el buen nombre o la intimidad, mejorar la aplicabilidad del consentimiento como una medida independiente y de segura protección al titular de los datos personales y finalmente una más acertada visibilidad de la Delegatura para la Protección de Datos de la Superintendencia como la entidad reguladora y protectora del derecho de habeas data.

REFERENCIAS

Agencia Española Protección de Datos. (2018, December 22). Elaborar el registro de actividades de tratamiento. Aepd. https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento

Aguirre, J. L. B. (Ed.). (2018). *Reglamento general de protección de datos novedades. Adaptación de la normativa española: El proyecto de LOPD* (Vol. 28, Issue Constitución y Convenio de Oviedo: aniversario de derechos). Fundación Dialnet.

Alarcón Peña, Andrea. (2018). Economía Social de Mercado como sistema constitucional económico colombiano. Un análisis a partir de la jurisprudencia de la Corte Constitucional. Estudios constitucionales, 16(2), 141-182. https://dx.doi.org/10.4067/S0718-52002018000200141

Angarita, N. R. (2012). Insuficiencia de la regulación latinoamericana frente a la recolección internacional da datos personales en internet. *Quaestiones Disputatae*, *2*, 181–226.

Ardila, B. Y. R. (2016). *Regulación en materia de protección de datos personales o habeas data en Colombia a través de la Ley 1581 de 2012: examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas*. Universidad Católica de Colombia.

Article 29 Data Protection Working Party. (2013). Opinion 03/2013 on purpose limitation. https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2013/wp203_en.pdf

Asunto C-553/07 College van burgemeester y wehouders van Rotterdam v MEE Rijkeboer, (2007). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0553

Botero, D. M. B. (2016). El valor de los datos personales en Colombia. *Revista CES Derecho*, 1–2.

Cavoukian, A. (2009). *Privacy By Design ... Take The Challenge*. INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO CANADA.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO - La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos . (2020). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0264

Concesión del anonimato a las partes en los procedimientos judiciales ante el Tribunal General de la Unión Europea, 1 (2019). https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-es-div-c-0000-2015-201508724-05_00.pdf

Data-driven law : data analytics and the new legal services / edited by Ed Walters - 1a Ed. - Boca Raton, Florida : CRC Press, 2019. - xi, 215 páginas - Data analytics applications series

de Datos, A. E. de P. (2020a). *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*. https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

de Datos, A. E. de P. (2020b). *Tecnologías y Protección de Datos en las AA.PP*. https://www.aepd.es/es/documento/guia-tecnologias-admin-digital.pdf

de Datos, A. E. P. la P. (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

De Hertab, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). T*he right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 11.* https://reader.elsevier.com/reader/sd/pii/S0267364917303333?token=B1CEAD082B942003940602996DD8BE20E17A11EBAB7C94E1BC4ED553CC9F039E501EF8A22FA0BEBF7BAE05CCFC4724FC&originRegion=us-east-1&originCreation=20220804173244

de Industria y Comercio, DP la P. de D.-S. (20 de abril de 2021). [Carta a Radicado 21-104275-].

de Industria y Comercio, S. (2014). *Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)*. https://issuu.com/quioscosic/docs/guia_accountability_26_p__g

de Industria y Comercio, S. (2018). *Resolución 12809 de 2018.* Superintendencia de Industria y Comercio. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE12809-2018.pdf

de Industria y Comercio, S. (2020). *Resolución Número 35093 de 2020*. Superintendencia de Industria y Comercio. https://www.sic.gov.co/sites/default/files/concepto-boletin-juridico/Resolucio%CC%81n%2035093%20del%206%20de%20julio%20de%202020%20UNE%20EPM.pdf

de Privacidad, E. (2020). *Guía comparativa del Reglamento General de Protección de Datos Europeo y el régimen Colombiano de protección de datos personales*. Escuela de Privacidad. https://escueladeprivacidad.co/wp-content/uploads/2020/05/Guia-Comparativa-Europa-Colombia.pdf

Decisión vinculante 1/2021 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con WhatsApp Ireland con arreglo al artículo 65, apartado 1, letra a), del RGPD . (s/f). Europa.eu. Recuperado el 10 de agosto de 2022, de https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_es

Decreto 1074 de 2015 - *Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Presidencia de la Republica* ___ (2015). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608

Gaceta del Congreso. (2010). *INFORME DE PONENCIA PARA SEGUNDO DEBATE AL PROYECTO DE LEY ESTATUTARIA NÚMERO 046 DE 2010 CÁMARA.* http://201.245.195.101 › 2010pdf › 488

Gaceta del Congreso. (2010a). *INFORME DE PONENCIA PARA PRIMER DEBATE AL PROYECTO DE LEY ESTATUTARIA NÚMERO 046 DE 2010 CÁMARA, 184 DE 2010 SENADO.* http://svrpubindc.imprenta.gov.co/senado/view/gestion/gacetaPublica.xhtml

Gaceta del Congreso. (2010b). *INFORME DE PONENCIA PARA SEGUNDO DEBATE AL PROYECTO DE LEY ESTATUTARIA NÚMERO 184 DE 2010 SENADO 046 DE 2010 CÁMARA*. http://svrpubindc.imprenta.gov.co/senado/index2.xhtml?ent=Senado&fec=13-12-2010&num=1080&consec=27771

Gaceta del Congreso. (2010c). *INFORME DE PONENCIA PARA SEGUNDO DEBATE AL PROYECTO DE LEY ESTATUTARIA NÚMERO 184 DE 2010 SENADO 046 DE 2010 CÁMARA.* http://svrpubindc.imprenta.gov.co/senado/index2.xhtml?ent=Senado&fec=13-12-2010&num=1080&consec=27771

Galvis Cano, L., & Salazar Bautista, L. R. (2018). *Alcance del derecho al olvido en el tratamiento de datos personales en Colombia. Verba Iuris, 41, 18.* https://doi.org/10.18041/0121-3474/verbaiuris.41.4647

García, L. R., & Pardo, B. H. (2018). *Protección de datos: la «seudoanonimización» inexistente. Fundación Dialnet, 28.* https://www.ajs.es/sites/default/files/2020-05/vol28n1_02_05_Estudio.pdf

GDPRHub. (2020). *Article 9 GDPR.* GDPRHub. https://gdprhub.eu/index.php?title=Article_9_GDPR

Gestiona Abogados. (2019, January 16). *INTERÉS LEGÍTIMO RGPD. Gestiona Abogados.* https://protecciondatoscertificado.es/interes-legitimo-rgpd%EF%BB%BF/

Grupo De Trabajo Sobre Protección De Las Personas En Lo Que Respecta Al Tratamiento De Datos Personales. (2014). *Dictamen 05/2014 sobre técnicas de anonimización*. https://www.aepd.es/es/documento/wp216-es.pdf

Jiménez, W. G. & Meneses, O. (2017). *Derecho e Internet: introducción a un campo emergente para la investigación y práctica jurídicas. Revista Prolegómenos Derechos y Valores , 20, 40, 43-61. DOI: http://dx.doi.org/10.18359/prole.3040*

Ley 1480 de 2011 - Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones, (2011). http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales, (2012). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Ley 906 de 2004 - Por la cual se expide el Código de Procedimiento Penal, (2004). http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

López Oliva, J., Vargas Chaves, I. & Alarcón Peña, A. (2022). La historia clínica: un medio de prueba estelar en los procesos de responsabilidad médica. Revista Jurídica Mario Alario D´Filippo, 14(27), 137–154. https://doi.org/10.32997/2256-2796-vol.14-num.27-2022-3813

López, A. (2018). El representante del responsable o del encargado del tratamiento de datos personales en la regulación actual. Diario La Ley, 9271

López-Oliva J., et-al (2017), La garantía de la protección del habeas data a través de la codificación procesal constitucional concentrada, en Procesal Constitucional: Codificación procesal Constitucional pp. 609 – 626, Ediciones Nueva Jurídica.

López-Sáez, M. M. (2017). *Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de*

datos personales. Estudios de Deusto, 65(2), 38. https://revista-estudios.revistas.deusto.es/article/view/1378/1659

Manzanero Jiménez, L., Pérez García-Ferrería J., (2016). Sobre el derecho al olvido digital: una solución al conflicto entre la libertad de información y el derecho de protección de datos personales en los motores de búsqueda. Revista Jurídica Universidad Autónoma De Madrid, (32). Recuperado a partir de https://revistas.uam.es/revistajuridica/article/view/6443

Martínez-Martínez, D.-F. (2018). Unificación De La Protección De Datos Personales En La Unión Europea: Desafíos E Implicaciones. *Revista internacional de Información y Comunicación*, 1–10.

Monsalve, V. (2015). análisis del contrato electrónico y la información pre y poscontractual en Colombia a propósito de la legislación comunitaria y extranjera. Revista Prolegómenos. Derechos y Valores, 18, 35, 17-48.

Monsalve, V. M. (2017). La protección de datos de carácter personal en los contratos Electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. *Revista Prolegómenos - Derechos y Valores*, 163–195.

Nuevo reglamento de protección de datos de carácter personal : medidas de seguridad / Emilio del Peso Navarro... [et al.] - Madrid : Díaz de Santos, 2008. - lii, 820 p.

Ortigosa, A. P. (2019). *DECISIONES AUTOMATIZADAS EN EL RGPD. EL USO DE ALGORITMOS EN EL CONTEXTO DE LA PROTECCIÓN DE DATOS. Revista General de Derecho Administrativo*, 50, 35. https://roderic.uv.es/bitstream/handle/10550/80448/RGDA.pdf?sequence=1&isAllowed=y

Peña, D. (2021), La protección de datos personales, entre lo público y lo privado, Universidad Externado, blog de derecho de los negocios, 2021. https://dernegocios.uexternado.edu.co/la-proteccion-de-datos-personales-entre-lo-publico-y-lo-privado/

Pucinelli , O. (2004), La protección de datos de carácter personal, Astrea, Buenos Aires, 2004.

Reglamento General de la Protección de Datos, 28 Reglamento UE 2016/679 88 (2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reigada, A. T. (2012). *El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 8, 38.* https://dialnet.unirioja.es/servlet/articulo?codigo=7505133

Savaris, J. A. (2012). Globalización, Crisis Económica, Conse-cuencialismo y la aplicación de los Derechos Económicos, Sociales y Culturales (DESC). Revista Prolegómenos. Derechos y Valores, 15, 30, 21-44

Sentencia C-748/11, Corte Constitucional De Colombia ___ (2011). https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Sentencia SU-082 De 1995, Corte Constitucional De Colombia ___ (1995). https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Sentencia SU458/12, Corte Constitucional De Colombia ___. https://www.corteconstitucional.gov.co/RELATORIA/2012/SU458-12.htm

Sentencia T-020/14, Corte Constitucional De Colombia ___ (2014). https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm

Sentencia T-443-94, Corte Constitucional De Colombia ___ (1994). https://www.corteconstitucional.gov.co/relatoria/1994/T-443-94.htm#:~:text=Este%20derecho%20otorga%20a%20la,abusen%20del%20derecho%20a%20informar.

Superintendencia de Industria y Comercio, O. A. J. (2018). *Consulta SIC Radicación: 18-171259-1*.

Taylor, Mark. (2021) *Genetic data and the law : a critical perspective on privacy protection - New York : Cambridge University Press, 2012. - xii, 232 p.* The critique. The consequence.

Villalba Cuéllar, J. (2008), Contratos por medios electrónicos, sspectos sustanciales y procesales, Prolegómenos. Derechos y Valores, vol. XI, núm. 22, julio-diciembre, 2008, pp. 85-108.