Tratamiento de datos personales y *compliance* en Colombia

Personal data processing and compliance in Colombia[1]

Juan Sebas ián Cabezas Azuero

Magíster en Derecho
Colegio Mayor de Nuestra Señora del Rosario – Colombia
juan.cabezas@urosario.edu.co
ORCID: https://orcid.org/0000-0002-2431-9417

Resumen

Este es un artículo de reflexión sobre el tratamiento de datos en Colombia por parte de las organizaciones empresariales. En él se ilustra el marco normativo de cumplimiento o *compliance* que debe seguirse para ajustarse a los lineamientos generales de protección de datos personales. El objetivo principal es la visualización del panorama de obligaciones del empresariado colombiano para el cumplimiento de la normativa de tratamiento de datos personales, teniendo en cuenta no solo los más recientes pronunciamientos de la autoridad nacional en la materia, sino también factores organizacionales como el tamaño o actividad económica de la empresa. Con esto se pretende generar espacios de conocimiento y discusión frente a un tema relativamente nuevo para el país.

Palabras clave

Datos personales, *compliance*, *habeas data*, principio de responsabilidad demostrada, derecho corporativo.

1 Artículo de reflexión producto de la investigación dirigida por el profesor Édgar Iván León Robayo como trabajo de grado para optar por el título de Magíster en Derecho con énfasis en Derecho Privado del Colegio Mayor de Nuestra Señora del Rosario.

Abstract

This is a reflection paper about personal data processing by companies in Colombia. It illustrates the compliance regulatory framework that must be followed to comply with the general guidelines for the personal data protection. The main objective is to visualize the panorama of obligations of the Colombian business community to comply with the regulations on the processing of personal data, considering not only the most recent declarations of the national authority, but also organizational factors such as size or economic activity of the company. This is intended to generate spaces for knowledge and discussion on a relatively new issue for the country.

Key words

Personal data, compliance, habeas data, accountability, corporate law.

Introducción

La correcta administración de los datos personales presenta para las organizaciones empresariales uno de los mayores retos en la era moderna. En efecto, la automatización en la forma de acceder a los datos, supone una alta responsabilidad para garantizar no solo los derechos de los titulares de los datos, sino también el cumplimiento de los principios que rigen la protección de datos personales tales como los de finalidad, libertad, seguridad, entre otros, mediante su correcto tratamiento, el cual, según el literal "g" del artículo 3 de la Ley 1581 de 2012, se entiende como *cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*. Estas obligaciones concernientes al tratamiento de datos personales tomaron por sorpresa al sector empresarial al momento de su entrada en vigor por desconocimiento de su alcance, razón por la cual su aplicación ha sido más lenta y sólo otorgándose relevancia al momento de sufrir incidentes particulares.

Cómo citar este artículo:
Cabezas Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de la Facultad de Derecho y Ciencias Políticas*, 53(138), pp. 1-25.
doi: https://doi.org/10.18566/rfdcp.v53n138.a2
Recibido: 05 de diciembre de 2022
Aprobado: 31 de mayo de 2022

No obstante, con el transcurso del tiempo se hizo evidente que estas obligaciones eran una realidad para las organizaciones empresariales de todos los sectores, ya que independientemente de su actividad económica, estas realizan en mayor o menor medida algún tipo de tratamiento de datos, que en todo caso les permitirá identificar con mayor precisión los comportamientos de los consumidores, aumentando así su productividad e ingresos (Martínez, 2019). Por tal razón, el reto a nivel corporativo es inmenso en aras de garantizar a los titulares el adecuado tratamiento de sus datos personales recolectados.

A través del Plan Nacional de Desarrollo 2010-2014 (Ley 1450, 2011), Colombia se propuso ingresar al grupo de países miembros de la Organización para la Cooperación y el Desarrollo Económico (en adelante OCDE), con la finalidad de generar un mejor posicionamiento del país a nivel mundial y beneficiarse de experiencias en la formulación de políticas públicas por parte de las economías líderes del mundo. Por esta razón, en materia del tratamiento de datos personales, distintas entidades gubernamentales como el Ministerio de Tecnologías de la Información, la Comisión de Regulación de Telecomunicaciones y la Superintendencia de Industria y Comercio (en adelante SIC), plantearon el marco normativo necesario que le permitieran al país cumplir con las directrices y buenas prácticas que promueve dicha Organización.

Así las cosas, el país cuenta ya con un marco normativo propio para el tratamiento de datos personales, que aplica a todas las actividades económicas, sin excepción alguna, y por el cual se establecen reglas que crean derechos, deberes y obligaciones para sus actores. No obstante, Colombia se encuentra en mora de actualizar su régimen legal para hacerlo compatible con el actual entorno digital que nos rodea: internet, *big data*, inteligencia artificial, centros de datos y ciberseguridad (Galvis & Salazar, 2018).

Aprobadas las primeras leyes en la materia (las cuales se detallan más adelante), el país se vio inmerso de un momento a otro en una regulación normativa poco socializada y desconocida por la mayoría. En el ámbito empresarial, la regulación se conoció a destiempo, bajo la idea que sólo era aplicable para empresas que tuvieran dentro de su actividad principal algún tipo de tratamiento de datos personales. Como consecuencia de ello, su aplicación por parte de las empresas ha sido lenta, desprovista de interés y considerada como una carga regulatoria que obstaculiza el desarrollo de su actividad económica.

No obstante, el marco normativo sobre el tratamiento de datos personales en Colombia aplica a todos los sectores económicos, públicos o privados, con algunas excepciones contenidas en el artículo 2 de la Ley 1581 de 2012, estableciéndose así en cabeza de las empresas un deber irrefutable para dar aplicación a la misma, permitiendo que el país se ajuste a los parámetros de la OCDE, y más importante aún, garantizando al Titular del dato la protección de los datos personales que obtienen en desarrollo de su actividad económica.

Es a través del cumplimiento normativo o *compliance* que las empresas encuentran respuesta a este requerimiento legal, estableciendo los parámetros necesarios para que en el ejercicio de su actividad económica se cumplan las disposiciones legales. Por tal razón, el presente escrito reflexiona sobre la aplicación de un correcto *compliance* en materia de tratamiento de datos personales, con el fin de hacer visible las obligaciones y deberes de las empresas, y los retos que supone su implementación, todo ello acompañando de pronunciamientos por parte de la Superintendencia de Industria y Comercio como autoridad nacional en la materia, quien, en cumplimiento de las competencias asignadas, profiere sanciones económicas y administrativas.

Lineamientos internacionales en materia de datos personales

La relevancia de los datos personales se hizo evidente a partir de la segunda mitad del siglo XX. En efecto, el surgimiento de la tecnología de las telecomunicaciones y el creciente comercio internacional postguerra, creó el ambiente propicio para el aumento en la recolección de datos personales, que pronto entraría en conflicto con el derecho a la intimidad de las personas. Por esta razón, la OCDE generó por primera vez unos lineamientos sobre la materia a través de la Guía denominada "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" (1980), la cual es resultado de la recomendación del Consejo de la OCDE frente al advenimiento de la tecnología de la información en diversos ámbitos de la vida económica y social, así como al creciente uso del procesamiento informático de datos. Por tal razón, a través de esta Guía, se reconoce la necesidad de proteger la privacidad y libertades individuales, las cuales no pueden verse en desmedro por el creciente tratamiento automático y flujo transfronterizo de datos personales con las nuevas formas de relaciones comerciales.

Esta Guía pretende, entonces, hacer frente a la intensificación en las operaciones comerciales con datos personales, principalmente para evitar su uso indebido o difusión no deseada, así como regular las obligaciones a cargo de los responsables en el tratamiento de datos. Para ello, dentro de su contenido, dispone de unos principios y reglas de implantación en la normativa nacional de los países para unificar criterios en la materia. Si bien su aplicación no es legalmente vinculante para los países, sí pretende generar unos lineamientos básicos que deben tener en cuenta las legislaciones internas de cada país para tener una regulación acorde con el tratamiento de datos; por lo tanto, por medio de esta primera versión, el organismo internacional sienta las bases acerca de la necesidad del *compliance* en la recolección de información personal de terceros por parte de las empresas, siendo esto una regulación visionaria, ya que a medida que se desarrollaban las tecnologías de la información, el tratamiento de datos lograría hacerse de manera masiva y automática como sucede en la actualidad.

La Guía de 1980 se ajusta a través del *The OECD Privacy Framework* (2013), con el fin de estar a tono con las nuevas realidades tecnológicas y generar así lineamientos modernos. En efecto, el organismo internacional evidencia que existen profundos cambios en la forma en que los datos personales actúan en la economía, la sociedad y en la vida diaria en general, debido principalmente al surgimiento del internet, al creciente flujo de información por medios digitales, a la expansión del comercio internacional, entre otros. Debido a estos cambios, se observa en el mundo un mayor volumen de datos personales recolectados, usados, almacenados y transferidos, haciéndose evidente el mejoramiento en los distintos niveles de análisis y su capacidad de tratamiento, lo que conlleva a la inminente violación de la privacidad de las personas, debido al gran número de actores que interactúan.

Entonces, a partir de esta revisión, se cuenta con un estudio mucho más elaborado y aplicable al estándar actual de desarrollo tecnológico, lo cual permite a los países unificar criterios para su implementación normativa nacional, y con ello contar con unas normas claras que permitan el desarrollo efectivo del *compliance* en las empresas.

A nivel europeo, también se ha expedido normativa desde la segunda mitad del siglo XX relacionada con el tratamiento de datos personales. La primera de ellas fue el Convenio 108 (1981) expedido por el Consejo de Europa, por medio del cual se establecen reglas en dicha región frente al tratamiento automatizado de datos personales de carácter personal, fijando pautas para

un modelo común de protección. Más adelante se expediría la Directiva 95/46/CE (1995) del Parlamento Europeo y del Consejo, por medio de la cual se desarrolla con mayor profundidad la materia, ampliando su aplicación a la protección de personas físicas frente al tratamiento de datos personales y su libre circulación, tanto al sector público como al privado. Así, esta Directiva establece unos criterios estrictos para la recolección y utilización de datos personales, solicitando además a cada Estado miembro de la Unión Europea, la creación de un órgano nacional independiente que vele por la protección de los datos personales de las personas.

Finalmente, se expide el Reglamento (UE) 2016/679 (2016) del Parlamento Europeo y del Consejo (RGPD), que avanza mucho más en el desarrollo de la materia, convirtiéndose en una norma vanguardista por su nivel de evolución y actualidad, ya que se concibió pensando en un entorno digital, con la finalidad de homogeneizar y dotar de coherencia a la normativa relacionada con el tratamiento de datos personales (Martínez-Martínez, 2018), aplicándose a empresas y organizaciones en la actividad de recolección, almacenamiento y gestión de datos personales.

Algunos puntos importantes del Reglamento se refieren a la necesidad de obtener consentimiento expreso y claro de los ciudadanos para que puedan tratarse sus datos personales (artículo 7°), establece la obligación de proporcionar información transparente por parte de las empresas (artículo 12°), desarrolla los derechos de acceso (artículo 15°), de rectificación (artículo 16°), de supresión (derecho al olvido) (artículo 17°), de portabilidad de datos (artículo 20°), de oposición (artículo 21°), crea el cargo del delegado de protección de datos personales al interior de las empresas (Sección 4 – artículos 37° a 39°), entre otros.

Ahora bien, con ocasión a la expedición de RGPD, se hace necesario analizar con mayor detenimiento el principio de territorialidad en su aplicación (Directriz 3/2018, *European Data Protection Board*), con el fin de identificar los eventos en que las empresas colombianas puedan ser objeto de esta. Así pues, de acuerdo con lo establecido en el artículo 3 del RGPD, el ámbito territorial de aplicación se define por dos criterios, a saber: el apartado 1 define el criterio del "establecimiento", mientras que el apartado 2 hace referencia al criterio de la "selección de destinatarios".

El primero de ellos, esto es el criterio del "establecimiento", determina que "el Reglamento se aplica al tratamiento de datos personales en el contexto de

las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no". Para detallar un poco más este criterio, deberá analizarse a través de un triple enfoque:

i) ¿qué se entiende por establecimiento en la Unión?, al respecto, el considerando 22 del RGPD indica que:

> "(…) un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto (…)"

ii) ¿el tratamiento de datos personales se realiza en el contexto de las actividades del establecimiento?, resulta de vital importancia la respuesta a este interrogante, ya que el solo hecho de contar con un establecimiento en la UE no puede considerarse suficiente para efectos de la aplicación del RGPD. Si bien se sugiere revisar caso por caso, se consideran factores determinantes la relación indisociable entre el tratamiento de datos personales del responsable o encargado por fuera de la Unión con la actividad de su establecimiento en la Unión, así como la recaudación de ingresos por parte del establecimiento en la Unión con ocasión al tratamiento de datos realizado por fuera de la Unión

iii) ¿el tratamiento de datos debe tener lugar en la Unión o no?, frente a este interrogante, el RGPD dispone que el lugar donde se realice el tratamiento de datos personales no es pertinente para determinar su aplicación, sino que lo es el hecho de hacerlo a través de un establecimiento en la UE en el contexto de sus actividades, lo cual además permite concluir que bajo el artículo 3, apartado 1, la aplicación del RGPD no se limita exclusivamente a particulares que residan en la UE.

Por su parte, el criterio de "selección de destinatarios" determina que el RGPD:

> "(…) se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión (…)".

Bajo este criterio, el RGPD prevé que la ausencia de un establecimiento en la UE no significa necesariamente que las actividades de tratamiento de datos personales por parte de un responsable o encargado en un tercer país queden excluidas de su aplicación. Con el fin de ahondar un poco más en el entendimiento de este criterio, se sugiere analizar con otro triple enfoque:

i) ¿quiénes se consideran interesados que residan en la UE?, bajo este enfoque se quiere hacer entender que el RGPD se aplica a toda persona que resida en la UE, sin limitar su protección a criterios de nacionalidad u otro tipo de estatus jurídico del interesado.
ii) Oferta de bienes y servicios, independientemente de que se requiera un pago o no, a interesados que se encuentren en la UE. Si bien el análisis depende caso por caso, podrán identificarse algunos factores como lo son el uso de la lengua o moneda distinta al del país del comerciante en la oferta de los bienes o servicios, por una lengua o moneda de la UE, así como la entrega de los bienes en Estados miembros de la UE, entre otros.
iii) El control del comportamiento de los interesados, esto es, que dicho control se produzca dentro del territorio de la Unión Europea, como en el caso de los seguimientos realizados a través de dispositivos móviles

El ámbito territorial es de importancia al identificar las sanciones que contempla el RGPD por su incumplimiento. El artículo 83 y 84 de dicho estatuto prevé las condiciones para la imposición de multas administrativas y sanciones, indicando que la supervisión de su aplicación corresponde a las autoridades de control de los Estados miembros y no de una autoridad de control única europea (De Miguel Asensio, 2017). Así mismo, se crea el Comité Europeo de Protección de Datos como el organismo único europeo, encargado de velar y arbitrar por los mecanismos de coherencia de aplicación del RGPD entre las autoridades de control de los Estados miembros, emitiendo decisiones de carácter vinculante (Martínez-Martínez, 2018), así como la de elaborar las directrices acerca de cómo deben ser interpretados los artículos y conceptos del RGPD (Gascón, 2021).

Una última mención en los lineamientos internacionales, la haremos al *Privacy Framework*, proferido en el marco de la *Asia Pacific Economic Cooperation* (2004). Este acuerdo económico, conformado por 21 economías de la región Asia-Pacífico, que se enfoca en la apertura de mercados y en la reducción de obstáculos al libre comercio e inversión, planteó la creación de un Marco de Privacidad flexible para regular el libre flujo transfronterizo de información que evitara la creación de barreras innecesarias, poniendo

sobre la mesa la importancia de proteger la privacidad de la información, pero manteniendo su flujo constante entre los miembros de la región económica Asia-Pacífico.

En ese sentido, se considera que su estándar de protección es menor al establecido por la OCDE o por la Unión Europea, ya que parte de un código de conducta voluntario que debe ser acogido por los responsables de tratamiento de datos mediante la certificación que otorguen unos agentes certificadores, y en la cual se deje constancia del cumplimiento de los principios establecidos en dicho Marco de Privacidad. Esto, con el fin que la obligación no implique trabas en el comercio internacional mediante las transacciones entre los distintos países, más aún, teniendo en cuenta las diferencias culturales, económicas y de regímenes legales tan arraigadas de cada uno de los miembros.

Marco normativo de los datos personales en Colombia

Colombia cuenta con un importante marco normativo en materia de datos personales, que permite al país tener un panorama claro sobre el desarrollo del *compliance* en la materia. La primera norma que la consagra es el artículo 15 de la Constitución Política, al establecer el *habeas data* con el rango de derecho fundamental. El *habeas data* es entendido como "la facultad de los individuos para rectificar, modificar, actualizar y, en términos generales, acceder a la información que sobre él se trate en una base de datos" (Calle, 2009). Este concepto se encamina, entonces, a definir la autodeterminación de los individuos en la disposición de su información personal, especialmente en relación con la conservación, uso y circulación. Para la Corte Interamericana de Derechos Humanos, el derecho al *habeas data* comprende las siguientes premisas:

1. El derecho de cada persona a no ser perturbado en su privacidad
2. El derecho de toda persona a acceder a información sobre sí misma en bases de datos públicos y privados para modificar, anular o rectificar información sobre su persona por tratarse de datos sensibles, falsos, tendenciosos o discriminatorios
3. El derecho de las personas a utilizar la acción de habeas data como mecanismo de fiscalización (CIDH, 2000).

   La primera normativa de rango legal que trata temas de habeas data es la

Ley Estatutaria 1266 de 2008. Si bien su intención, desde el proyecto de ley, era convertirse en una ley que consagrara los principios generales a todo tipo de tratamiento de datos personales, su alcance solo se limitó a la protección del dato financiero y comercial, constituyéndose así en una regulación de tipo sectorial.

Y es que, en efecto, desde el artículo primero se evidencia que su objeto es delimitar la regulación al tratamiento de datos personales de carácter crediticio, financiero, comercial y de servicios, así como el cálculo del riesgo crediticio, enfocándose en el desarrollo de una actividad de interés público como es la actividad financiera, por cuanto sirve de soporte para la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad de este. Esto ratificado por la Corte Constitucional en el análisis de constitucionalidad de la norma, al expresar que:

> El proyecto de ley estatutaria objeto de examen constituye una regulación parcial del derecho fundamental al hábeas data, concentrada en las reglas para la administración de datos personales de naturaleza financiera, crediticia, comercial, de servicios y la proveniente de terceros países con idéntica naturaleza destinados al cálculo del riesgo crediticio, razón por la cual no puede considerarse como un régimen jurídico que regule, en su integridad, el derecho al hábeas data. El ámbito de protección del derecho fundamental al hábeas data previsto en el Proyecto de Ley, se restringe a la administración de datos de índole comercial o financiera, destinada al cálculo del riesgo crediticio, con exclusión de otras modalidades de administración de datos personales (Sentencia C-1011 de 2008).

Debido a lo anterior, el país aún se encontraba en mora de expedir una normativa general sobre los datos personales en Colombia. Por esta razón, es que la expedición de la Ley 1581 de 2012 se convierte en el régimen general de protección de datos personales, ya que su objeto es desarrollar el derecho que tienen las personas a "(…) conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política (…)" (Ley 1581, 2012, artículo 1). Con la entrada en vigencia de esta ley, las empresas que desarrollen cualquier actividad económica asumen obligaciones frente a la protección y tratamiento de datos personales que obtengan de las personas en general, ya sean empleados, clientes, proveedores, socios, o cualquier otro tercero.

Ahora bien, los deberes generales a cargo de los Responsables de tratamiento de datos se consagran en el artículo 17 de la Ley 1581 de 2012, entre los cuales se encuentran los de desarrollar políticas de tratamiento de la información ajustada a sus necesidades, solicitar autorización a los titulares al momento de obtener los datos personales, garantizar a los titulares los derechos allí consagrados y ofrecer los canales apropiados para que se puedan presentar consultas o elevar quejas relacionadas con la información entregada. Adicionalmente, las empresas tienen el deber de inscribirse en el Registro Nacional de Bases de Datos. Así las cosas, la Ley 1581 ofrece un marco completo para una correcta aplicación del derecho al *habeas data* y, por ende, para el desarrollo de un *compliance* efectivo al interior de las empresas, ratificado esto por la Corte Constitucional en el estudio de constitucionalidad de esta:

> Ahora, con el nuevo proyecto de ley se busca llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que su título sea precisamente "Por el cual se dictan disposiciones generales para la protección de datos personales", concluyéndose que con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato. (Sentencia C-478 de 2011)

Como regulación a la Ley 1581, el Gobierno Nacional expide el Decreto Reglamentario 1377 de 2013 (actualmente contenido dentro del Decreto Compilatorio 1074 de 2015), por medio del cual se dispone con mayor precisión de las obligaciones a cargo de las empresas frente al tratamiento de datos personales, siendo algunos de estos aspectos los relacionados con el procedimiento para obtener autorización del titular de datos, el contenido mínimo de las políticas de tratamiento de datos personales, la transferencia y transmisión de datos personales y el principio de responsabilidad demostrada.

En asocio con la normativa mencionada, no puede pasarse por alto la Ley 1273 de 2009 por medio de la cual se adiciona el Código Penal consagrando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", regulándose de manera taxativa los delitos informáticos.

Por medio de esta, se busca otorgarle protección penal a todo tipo de atentado a la confidencialidad, integridad y disponibilidad de datos y sistemas

informáticos, ya sea por el acceso abusivo a los sistemas, obstaculización ilegítima, interceptación de datos informáticos o uso de software malicioso; así, por medio de la Ley 1273 se reconoce la vulnerabilidad de los sistemas informáticos y la posible afectación de los datos personales recolectados, consagrando de esta forma penas privativas de la libertad y de índole económica como medidas preventivas y sancionatorias a la comisión del delito.

Todo este marco normativo deberá actualizarse para hacerlo coherente con el nuevo entorno digital al que nos vemos sujetos diariamente. En efecto, la llegada de nuevas tecnologías de la información demuestra la necesidad de renovar la normatividad para mitigar los riesgos de los titulares de datos frente a su derecho a la privacidad, relacionada por ejemplo con tratamiento malintencionado del rastro o huella digital o actividades de ciber-acoso, así como para lograr un ámbito de aplicación mayor para cubrir el tratamiento de datos personales en medios ubicados fuera del país (Martínez, 2019).

Cumplimiento normativo o *compliance* en materia de datos personales

El *compliance* es conocido como una de las nuevas prácticas del derecho, por medio del cual se pretende generar una autorregulación empresarial en el desarrollo de su actividad económica, garantizando el cumplimiento normativo al que se encuentran obligados a través del establecimiento de códigos internos de conducta. Según la doctrina, el *compliance* parte de la creación de modelos de prevención y manejo de riesgos "(…) a través de la introducción de una cultura del respeto de las normas legales y éticas en las empresas, que implica el establecimiento de códigos de conducta, medidas de autovigilancia, controles y la determinación de los flujos de información" (Castro & Perdomo, 2018). Para que sea efectivo, el *compliance* conlleva un análisis integral de distintas situaciones al interior de la empresa, para materializarlas a través de la implementación y vigilancia de sus procedimientos internos. Para ello, las empresas deben ceñirse a unos códigos de ética y conducta que garanticen equidad y transparencia en sus procesos de rendición de cuentas, en sus decisiones frente a terceros y en sus relaciones comerciales.

En Colombia, hoy en día encontramos actividades de *compliance* en materia de lavado de activos, lucha contra la corrupción, riesgos ambientales y sanitarios, protección de datos personales, entre otras. Así, en la materia que nos atañe, el *compliance* hace referencia a los procedimientos y organización

al interior de una empresa, que garanticen el cumplimiento de la normativa relacionada con el tratamiento de datos personales, mediante el control y vigilancia interna, con el fin de hacer efectivo el derecho constitucional al habeas data con el que cuentan las personas.

A continuación, analizaremos los deberes de los "responsables" contenidos en el marco normativo nacional, con el fin de detallar los lineamientos para el desarrollo del *compliance* en esta materia, asimismo, de manera simultánea, haremos referencia a algunos retos actuales que supone la implementación de un programa de cumplimiento normativo organizacional relacionado con el tratamiento de datos.

En primera medida, todo "Responsable" y/o "Encargado" del tratamiento de datos deberá designar a una persona o área que asuma la función de protección de datos personales. Este cargo, conocido como Oficial de Protección de Datos, tiene como función velar por la implementación efectiva de las políticas y procedimientos adoptados por la organización para el cumplimiento del marco normativo en materia de datos personales, así como lograr la implementación de buenas prácticas de gestión de dichos datos al interior de la organización. De entrada, evidenciamos el que puede ser uno de los mayores retos para las organizaciones, y es el hecho de disponer de recursos económicos, físicos y humanos, adicionales a su negocio o actividad económica, para el desarrollo del cargo del "Oficial de Protección de Datos". Y es que, en efecto, la implementación de este tipo de programas de seguimiento de cumplimiento normativo supone para los "Responsables" un compromiso a nivel gerencial para el desembolso de estos recursos, que permitirán materializar la creación y seguimiento al programa.

En consonancia con lo anterior, existe un desconocimiento generalizado del marco normativo de protección de datos personales por parte de las organizaciones empresariales. Y esto toma relevancia por cuanto la asignación de recursos atrás mencionada, debe primero partir de explicar y dar a conocer el marco normativo al interior de las organizaciones, quienes podrán no darle mayor importancia al tratarse de un tema por fuera de su actividad negocial principal. Lo anterior supone la existencia de verdadero riesgo de incumplimiento al marco normativo, que finalmente se replicará en las facultades sancionatorias de la autoridad nacional en la materia, esto es la Superintendencia de Industria y Comercio.

Esto sumado al hecho de que para las organizaciones cuyas actividades trascienden fronteras nacionales, deberán enfrentarse igualmente a regímenes legales distintos, como por ejemplo verse sujetas a la aplicación del RGPD, según los criterios expuestos anteriormente, y que por ende deberán ajustarse a sus criterios, como lo son: la adopción de tecnologías que permitan la portabilidad de la información, la modificación y reestructuración de políticas organizacionales para el tratamiento de datos, ajustes de contratos y documentación mínima, aplicación de la normas ISO 27001 y adopción de medidas de gestión enfocadas en el tratamiento de datos personales (Ortiz, 2019). En ese sentido, el desarrollo del *compliance* bajo estas condiciones es aún más exigente, ya que supone ajustarse a distintas regulaciones legales y autoridades de control, para lo cual es evidente que deben asignarse mayores recursos al interior de la organización.

Ahora bien, la creación del programa interno de cumplimiento normativo conlleva la generación de distintos documentos que permiten materializar el tratamiento de datos personales. En primera medida, encontramos el "Manual de Políticas y Procedimientos Internos" para el tratamiento de datos personales, en el cual se expliquen todos los parámetros que sigue la compañía para garantizar el buen uso de estos, tales como mapa de riesgos, interacciones de las distintas áreas, procedimientos internos para la atención de quejas, consultas y reclamos que presenten los titulares de datos personales en atención a su derecho al habeas data, entre otras (Superintendencia de Industria y Comercio, 2022). El objetivo de este manual es demostrar:

i) La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable, para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y el Decreto 1377 de 2013
ii) La adopción de mecanismos internos para poner en práctica las políticas, incluyendo herramientas de implementación, entrenamiento y programas de educación
iii) La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

Sin importar su tamaño, total de activos o empleados, toda empresa que realice tratamiento de datos personales se encuentra en la obligación de contar con este Manual debidamente documentado al interior de la compañía. Del mismo modo, está en la obligación de capacitar a sus colaboradores para un adecuado tratamiento de datos personales, esto es de generar compañas

educativas de entrenamiento al personal que se encuentre con mayor inmediatez frente al manejo de datos, con lo cual se pretende disminuir el riesgo de incumplimiento por desconocimiento de la normatividad. En ese sentido, la SIC manifiesta:

> La sociedad en calidad de Responsable del Tratamiento no solo debe implementar un manual interno de políticas y procedimientos para la atención de quejas y reclamos sino que los términos establecidos en el mismo no debe ser superiores a los dados en los artículos 14 y 15 de la Ley 1581 de 2012 y en virtud del principio de responsabilidad demostrada, deben ser puestos en conocimiento y socializados con todo el personal que atienda las consultas y reclamos" (Superintendencia de Industria y Comercio, 2019).

Adicional a las políticas internas, las compañías se encuentran en la obligación de contar con una Política de Tratamiento de Datos Personales, que es aquel documento al cual podrán acceder los titulares para verificar el tratamiento que se hará a sus datos personales.

Estas políticas requieren de un contenido mínimo, consagrado en la ley, por medio del cual se pretende garantizar al titular toda la información necesaria para comprender en su totalidad el tratamiento por realizar. Dicho contenido mínimo comprende:

i) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del "Responsable" del tratamiento de los datos
ii) Tratamiento al cual serán sometidos los datos y finalidad del mismo, cuando no se haya informado mediante aviso de privacidad
iii) Derechos que tiene el titular de la información
iv) Persona o área responsable de la atención de peticiones, consultas y reclamos, ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y/o revocar la autorización
v) Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización
vi) Fecha de entrada en vigor de la política de tratamiento de la información y período de vigencia de la base de datos
vii) Cualquier cambio sustancial en las políticas de tratamiento de datos personales debe ser comunicado oportunamente a los titulares de una manera eficiente, antes de implementar las nuevas políticas (Superintendencia de Industria y Comercio, 2017).

Además de esto, el "Responsable" tiene a su cargo la obligación de poner en conocimiento de los titulares esta política de tratamiento de datos personales, para lo cual se podrá valer de notificaciones por cualquier medio, ya sea tecnológico, presencial, verbal y/o cualquier otro medio que permita al titular conocer de dicha política. En otras palabras, no solo basta con la elaboración de las políticas, sino que también se encuentra a su cargo la obligación de publicitarlo a los titulares de datos sobre los cuales realiza tratamiento.

Ahora bien, debido a que algunas recolecciones de datos personales se realizan a través de formularios, con el fin de informar a los titulares de datos personales de la existencia de las políticas de tratamiento de datos personales, se permite entonces hacerlo a través del Aviso de Privacidad. En este sentido, el Aviso de Privacidad es uno de los medios de difusión por medio de los cuales el "Responsable" comunicará a los titulares de la existencia de las políticas de tratamiento de datos. Debido a que la finalidad del Aviso de Privacidad es prácticamente informativa, su contenido igualmente es bastante resumido. Requiere como mínimo contar con:

i) Nombre o razón social y datos de contacto del responsable del tratamiento
ii) Finalidad de la recolección de los datos y el tipo de tratamiento al que serán sometidos
iii) Derechos que tiene el titular de la información
iv) Mecanismos dispuestos por el "Responsable" de los datos para que el titular conozca la política y los cambios que se produzcan en ella o en el aviso de privacidad correspondiente (Superintendencia de Industria y Comercio, 2017).

Junto con los documentos antes mencionados, existe la obligación de contar con la respectiva Autorización por medio de la cual el Titular otorga consentimiento para el tratamiento de sus datos personales. La autorización, entonces, es un desarrollo del principio de libertad en materia de datos personales[2], siendo necesaria su obtención a más tardar en el momento de recolección de los datos, la cual debe ser además expresa e informada, esto es, que el titular tenga conocimiento para qué y cómo se utilizará la información personal recolectada (Corte Constitucional, sentencia C-478 de 2011).

2 Principio de Libertad: El tratamiento de datos personales solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. Recuperado de https://www.sic.gov.co/preguntas-frecuentes-pdp

Debe tenerse en cuenta que, los datos considerados como públicos pueden ser tratados sin necesidad de autorización por parte de su titular. El mismo artículo 5 de la Ley 1581 de 2012, señala que los datos personales que se encuentren en fuentes de acceso público pueden ser tratados por cualquier persona, siempre y cuando, por su naturaleza, sean datos públicos. Así las cosas, los datos de las personas contenidos en registros públicos, boletines oficiales o sentencias ejecutoriadas no sujetas a reserva, tales como estado civil, profesión u oficio, podrán ser tratados por las empresas sin necesidad de obtener autorización de su titular, siempre y cuando, se reitera, por su naturaleza tengan la categoría de públicos.

Esta autorización podrá obtenerse de manera verbal, escrita o por conductas inequívocas del titular que permitan concluir su autorización (artículo 7 decreto 1377), es decir, aquellas que no admiten duda o equivocación del titular, que permitan concluir de forma razonable que otorgó la autorización. Ejemplo de conducta inequívoca son los sistemas de auto vigilancia, en los que previamente a su ingreso al establecimiento, se le comunica al Titular de la toma de imagen, quien, a sabiendas de esto, autoriza e ingresa. Para obtener la autorización, el "Responsable" podrá valerse de mecanismos eficientes de comunicación masiva como correos electrónicos, carteles informativos, periódicos, o medios técnicos que faciliten al titular la manifestación automatizada. En todo caso, el hecho de guardar silencio por parte del Titular no podrá asimilarse a la conducta inequívoca de aceptación.

Ahora bien, sin importar el medio utilizado para obtener la autorización, resulta de la mayor importancia contar siempre con la prueba de su otorgamiento para posterior consulta del titular, ya que "en esta materia debe existir plena prueba de la voluntad inequívoca de la persona para permitir que terceros recolecten, usen, consulten o realicen cualquier actividad con su información" (Superintendencia de Industria y Comercio, 2020). Sin duda, otro de los grandes retos de las organizaciones, es mantener un repositorio o archivo de las autorizaciones para consulta, más aún en aquellos casos en los que la autorización se lleva a cabo por medios no digitales o automatizados.

La recolección de datos personales siempre debe tener una finalidad legítima y cierta, esto es, que exista un motivo por el cual se lleva a cabo su tratamiento. En otras palabras, es necesario que exista una relación de causalidad entre los datos personales recolectados y el fin que con los mismos se persigue. Es de resaltar, que no se permite el tratamiento de datos con

finalidades ilegítimas o que no sigan unos propósitos para los cuales fueron recolectados. En palabras de la Corte Constitucional:

> Debe resaltarse que, si bien la norma permite que el consentimiento se preste "en forma general", ello debe interpretarse de forma compatible con el principio de libertad, razón por la que tal modalidad de autorización deberá, en todo caso, manifestar la finalidad expresa respecto de la cual se autoriza el acceso a los datos personales por parte del usuario. Así, dicha generalidad se predicará de las distintas finalidades autorizadas, sin que signifique la legitimidad de una cláusula abierta, que no identifique claramente los propósitos para el citado acceso por los usuarios. En efecto, si bien la norma hace referencia a "cualquier otra finalidad", en todo caso exige que "se haya obtenido autorización por parte del titular de la información" (Sentencia C-1011 del 16 de octubre de 2008).

Por otra parte, las organizaciones tienen el deber de garantizar la seguridad de la información, esto es de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento por parte de terceros, lo cual cada día es más necesario debido a los grandes niveles de virtualidad a los que nos vemos sujetos en todos los ámbitos, desde el laboral hasta el comercial y personal, en donde los ataques cibernéticos son cada vez más frecuentes y los métodos de secuestro de información de las empresas ya no pueden considerarse extraños. En ese sentido, la SIC ha manifestado que:

> La debida administración de datos implica, entre otras cosas, garantizar el principio de seguridad. En otras palabras, el tratamiento de datos que desconozca ese principio no es consistente con la Constitución ni la ley. Ese tipo de administración no es admisible a la luz de la regulación colombiana y no puede convertirse en una práctica empresarial ni es tolerable por las autoridades que según el artículo 2 de la Constitución "están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades (Superintendencia de Industria y Comercio, 2019).

Es importante resaltar que, las empresas deberán tener en cuenta tanto la naturaleza como el volumen de los datos personales que tratan, con el fin de proporcionar medidas de seguridad eficientes y proporcionales. En tal sentido, no existe un estándar único sobre las medidas de seguridad, sino que, por el contrario, las mismas dependerán en cada caso en particular según distintas circunstancias que deben ser tenidas en cuenta. En todo caso, las medidas de

seguridad deben resultar eficaces en la práctica, y no sólo constituir políticas consignadas en el papel, por lo cual se constituye en una realidad que debe ser verificable y comprobable a la luz de la autoridad nacional.

Ahora bien, de suma importancia tener en cuenta que, al momento de sufrir algún tipo de falla en la seguridad de la información, el "Responsable" deberá reportarlo a la autoridad nacional en un plazo no mayor a 15 días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos (Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio). Esto con el fin de determinar los tipos de datos que sufrieron la falla de seguridad, y demostrar las medidas adicionales tomadas por el "Responsable" para mitigar el incidente de seguridad, minimizando los perjuicios materiales o inmateriales que puedan sufrir los titulares de la información.

Dependiendo del caso en particular, deberá notificarse el incidente de seguridad a los Titulares de datos, para que estos tomen medidas adicionales que salvaguarden su información. Finalmente, los "Responsables" deberán documentar al detalle el incidente para futuras ocasiones, así como realizar monitoreos de control que permitan actuar de forma rápida ante nuevos incidentes.

Por otro lado, los "Responsables" se encuentran en la obligación de inscribir sus bases de datos en el Registro Nacional de Bases de Datos. Su consagración exige que las personas naturales o jurídicas, de naturaleza pública o privada, que realicen tratamiento automatizado o manual de datos personales, deban hacer su inscripción en este registro que es administrado por la SIC. El registro implica la inscripción de todas y cada una de las bases de datos con las que cuenten las empresas, ya sea de clientes, colaboradores, proveedores, etc.

Ahora bien, de acuerdo con el Decreto 090 de 2018, se establecen unos criterios para definir las empresas sujetas a este registro, tanto por la totalidad de sus activos, como en el plazo para llevarlo a cabo. Con relación al primer criterio, el registro debe llevarse a cabo únicamente por las sociedad y entidades sin ánimo de lucro que tengan más de 100.000 UVT´s de activos totales (independiente del número de empleados) y las entidades públicas.

Frente al segundo criterio, esto es el plazo para registrarse, el Decreto estableció una serie de criterios que, en todo caso, no superaban el 31 de enero de 2019. Toda empresa creada con posterioridad al vencimiento de este plazo,

tendrán un plazo máximo para su inscripción de dos (2) meses a partir de su creación, constituyéndose así en uno de los nuevos puntos de cumplimiento para la creación de empresas.

Este puede ser considerado uno de los puntos más conflictivos para los empresarios a la hora de llevar a cabo el registro de sus bases de datos, toda vez que significa entregar a una entidad uno de sus activos más importantes como es la información comercial de clientes y proveedores. De acuerdo con la Circular 003 de 2018 de la Superintendencia de Industria y Comercio, se establece la información mínima que debe inscribirse en el RNBD, su procedimiento para llevar a cabo dicha inscripción en el portal web de esta entidad y la obligación de actualización de las bases de datos anualmente a más tardar el 31 de marzo o, en caso de cambios sustanciales en las bases de datos, dentro de los primeros 10 días hábiles de cada mes. En ese sentido, al corresponder todo a una información indispensables para las organizaciones, la SIC debe garantizar un nivel superior de administración de la información, con el fin de que la misma no sufra afectaciones que sirvan para realizar prácticas restrictivas al comercio o de competencia desleal.

Finalmente, todas las obligaciones anteriores confluyen en el principio de responsabilidad demostrada, por medio del cual se establece que está a cargo de las organizaciones, la aplicación de las medidas conducentes que permitan demostrar el cumplimiento de la normatividad relativa al tratamiento de datos personales. Así, no basta simplemente con cumplir las obligaciones atrás descritas, sino que además será necesario contar con un programa integral dentro de la compañía, con el fin de demostrar la implementación de medidas apropiadas para el cumplimiento de la normativa, de conformidad con:

i) La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente
ii) La naturaleza de los datos personales objeto del tratamiento
iii) El tipo de tratamiento
iv) Los riesgos potenciales que el referido tratamiento podría causar sobre los derechos de los titulares.

Por tal razón, la autorregulación de las empresas debe estar acompañada de herramientas que la hagan eficaz o demostrable. Para ello, debe contar con mecanismos de control interno y externo que permiten verificar su cumplimiento. De acuerdo con la SIC, la responsabilidad demostrada puede

ejecutarse bajo un Programa Integral de Gestión de Datos Personales (PIGDP), a través del cual se cumpla efectivamente con el principio de responsabilidad demostrada bajo los lineamientos de compromiso de la organización, control, evaluación, revisión y demostración. Lo anterior en concordancia con lo manifestado por la SIC, en el sentido en que el tratamiento de datos personales debe ser real y verificable, y no sólo axiológico, ya que en la mayoría de los casos se queda en documentos elaborados que no son fielmente puestos en práctica y que no cumplen su finalidad.

> El principio de responsabilidad demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre el tratamiento de datos personales. Ésta exige implementar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo dependerá del compromiso real de todos los miembros de una organización pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos (Superintendencia de Industria y Comercio, 2019).

Por consiguiente, la aplicación real del principio de responsabilidad demostrada se convierte en una herramienta fundamental para que la organización no se vea afectada por sanciones de carácter administrativo o judicial, que perjudiquen no solo sus arcas, sino también su reputación empresarial, por medio de la aplicación de estándares objetivos de actuación, que de antemano brinden certeza sobre el accionar sancionatorio de la autoridad nacional. De acuerdo con lo informado por la SIC, las sanciones que se habían impuesto para dicha fecha correspondían a:

i) Reportes a centrales de riesgo que no corresponde a la realidad
ii) No actualización oportuna de información
iii) No aviso al deudor antes de hacer el reporte a centrales de riesgo
iv) Utilización de información de personas con fines de mercadeo sin la autorización del titular
v) Fallas en la seguridad de la información que dan lugar a la divulgación de los datos en internet, incluso de datos sensible
vi) Hurto y/o pérdida de la información contenida en bases de datos, entre otras (Superintendencia de Industria y Comercio, 2017).

Debe tenerse en cuenta que, según el artículo 23 de la Ley 1581 de 2012, en caso de encontrarse fallas en el tratamiento de datos personales, la SIC impondrá sanciones a las empresas que pueden ser multas hasta por 2.000 smmlv, suspensión de actividades hasta por 6 meses, cierre temporal y definitivo de las operaciones que involucren el tratamiento de datos. Por tal razón, es de vital importancia la correcta implementación del *compliance* al interior de las compañías de acuerdo con lo manifestado por la SIC:

> Por tanto, las organizaciones deben "implementar el compliance" en su estructura empresarial con miras a acatar las normas que inciden en su actividad y demostrar su compromiso con la legalidad. Lo mismo sucede con "accountability" respecto del tratamiento de datos personales. La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del compliance y buena parte de lo que implica el principio de responsabilidad demostrada (accountability). En la mencionada guía se considera fundamental que las organizaciones desarrollen y ejecuten, entre otros, un "sistema de administración de riesgos asociados al tratamiento de datos personales" que les permita "identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales (Superintendencia de Industria y Comercio, 2020).

Conclusiones

Desde hace algunos años, se hace mención que la información de los datos personales recolectados puede ser catalogada como el nuevo petróleo para las organizaciones empresariales, toda vez que genera distintas expectativas de crecimiento económico a través de su explotación (*The Economist*, 2017). Así, el tratamiento de datos personales se convierte en una herramienta fundamental para el desarrollo económico de la empresa, el cual en un mundo cada vez más competitivo, surge como una nueva posibilidad que no puede pasarse por alto ni menospreciarse. No obstante, como contrapartida, la privacidad de las personas se encuentra en una delgada línea de vulnerabilidad, debido a la cantidad de medios por los cuales se recolectan los datos y las medidas de seguridad que se utilizan para evitar su alteración o divulgación no deseada.

En vista de lo anterior, Colombia emprendió un ajuste normativo en esta materia, que toca temas tan sensibles como la privacidad de la información de

las personas, teniendo como base principalmente los lineamientos planteados por la OCDE en los años 1980 y 2013 (Rojas, 2014). Por tal razón, el presente trabajo puso de presente no sólo el marco normativo actual, sino también su aplicación a nivel de *compliance* a través del desarrollo de los distintos elementos necesarios para llevarla de la teoría a la práctica, el cual en todo caso ha sido convulsionado para las organizaciones que no se encontraban capacitadas, y mucho menos contaban con el conocimiento y recursos necesarios para atender esta nueva obligación.

Como consecuencia de ello, nos encontramos en un escenario en el que las organizaciones empresariales deben ajustarse a la normatividad de datos personales en Colombia, con el fin de ejercer un correcto tratamiento a la información personal entregada por los titulares, y evitar así verse sujetas a sanciones por parte de la autoridad nacional en la materia; no obstante, llevar a cabo esta tarea es cuando menos dispendioso y costoso, toda vez que implica destinar presupuesto, recursos físicos y humanos, a una obligación que no se encontraba planificada con anterioridad. En todo caso, las empresas deben entenderlo no solo como una imposición, sino como una oportunidad, para, acogidos al sistema legal, realizar un correcto tratamiento de los datos personales de sus clientes y expandir sus posibilidades de nuevos negocios.

Referencias

Calle, S. B. (2009). *Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia*. Precedente. Revista Jurídica, (-), 119-136. DOI: https://doi.org/10.18046/prec.v0.1459

Castro Cuenca, C. y Ospina Perdomo, J. (2018). *Derecho Penal Societario*. Bogotá D.C. Editorial Universidad del Rosario.

Corte Constitucional (2008). Sentencia C-1011. M.P. Jaime Córdoba Triviño.

Corte Constitucional (2011). Sentencia C-748. M.P. Jorge Ignacio Pretelt Chaljub.

De Miguel Asensio, P. A. (2017). *Competencia y derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea*. Revista Española de Derecho Internacional. 69 (jun. 2017). 75-108. DOI: http://dx.doi.org/10.17103/redi.69.1.2017.1.03

Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. Organización para la Cooperación y el Desarrollo Económico (OCDE). https://www.oecd.org/sti/ieconomy/15590267.pdf

Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3). Versión 2.1. 12 de noviembre de 2019. *European Data Protection Board*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf

Galvis Cano, L. y Salazar Bautista, R. (2018). *Alcance del derecho al olvido en el tratamiento de datos personales en Colombia*. Revista Verba Iuris, 14 (41). pp. 45-63. DOI: https://doi.org/10.18041/0121-3474/verbaiuris.41.4647

Gascón Marcén, A. (2021). *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea*. Cuadernos de Derecho Transnacional. 13 (oct. 2021). 209-232. DOI: https://doi.org/10.20318/cdt.2021.6256

Informe Anual (2000). Relatoría para la Libertad de Expresión. Corte Interamericana de Derechos Humanos. http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202000.pdf

Martínez Devia, A. (2019). *La inteligencia artificial, el big bata y la era digital: ¿una amenaza para los datos personales?* Revista La Propiedad Inmaterial. *27* (jun. 2019), 5-23. DOI: https://doi.org/10.18601/16571959.n27.01.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2016). Diario Oficial de la Unión Europea L 119/1. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Rojas Bejarano, M. (2014). *Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.* Novum Jus, 8(1), 107-139. DOI: https://doi.org/10.14718/NovumJus.2014.8.1.6

Sanclemente-Arciniegas, J. (2020). *El derecho comercial: de la regulación al compliance.* Estudios Socio-Jurídico, 22(2), 1-30. DOI: https://doi.org.ez.urosario.edu.co/10.12804/revistas.urosario.edu.co/sociojuridicos/a.7958

Superintendencia de Industria y Comercio. (02 de julio de 2020). Resolución No. 34638. Superintendente Delegado para la Protección de Datos Personales. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE34638-2020.pdf

Superintendencia de Industria y Comercio. (25 de agosto de 2020). Resolución No. 50091. Superintendente Delegado para la Protección de Datos Personales. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Resoluci%C3%B3n%20No_%2050091%20de%2025%20de%20agosto%20de%202020%20(COLOMBIA%20TELECOMUNICACIONES%20S_A%20E_S_P_).pdf

Superintendencia de Industria y Comercio. (07 de marzo de 2019). Resolución No. 5477. Director de Investigación de Protección de Datos Personales. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE5477-2019.pdf

Superintendencia de Industria y Comercio. (2017) *Formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios*. https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

Superintendencia de Industria y Comercio. (24 de enero de 2019). Resolución No. 1321. Director de Investigación de Protección de Datos Personales. https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Superintendencia de Industria y Comercio. (31 de marzo de 2022). Resolución No. 17360. Director de Investigación de Protección de Datos Personales. https://www.sic.gov.co/sites/default/files/files/2022/RE17360-2022.pdf

Superintendencia de Industria y Comercio. (8 de junio de 2017). *Por violaciones de datos personales, Superintendencia a impuesto sanciones por más de $21 mil millones de pesos*. http://www.sic.gov.co/noticias/por-violaciones-de-datospersonales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-depesos

The Economist. (2017). *The world´s most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The OECD Privacy Framework (2013). OECD. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf