TRATAMIENTO DE DATOS PERSONALES Y LAS PLATAFORMAS DIGITALES
RESEÑA SOBRE COLOMBIA Y LA UNIÓN EUROPEA

TRABAJO DE GRADO PARA OPTAR POR EL TITULO DE ESPECIALISTA EN DERECHO COMERCIAL

PRESENTADO A DR. CAMILO ENRIQUE GÓMEZ LÓPEZ

PRESENTADO POR:

LAURA CAROLINA MANTILLA DE VALERA

PONTIFICIA UNIVERSIDAD JAVERIANA
ESPECIALIZACIÓN EN DERECHO COMERCIAL
Bogotá D.C., diciembre de 2019

TRATAMIENTO DE DATOS PERSONALES Y LAS PLATAFORMAS DIGITALES
RESEÑA SOBRE COLOMBIA Y LA UNIÓN EUROPEA

TABLA DE CONTENIDO

TRATAMIENTO DE DATOS PERSONALES Y LAS PLATAFORMAS DIGITALES RESEÑA SOBRE COLOMBIA Y LA UNIÓN EUROPEA

1. INTRODUCCIÓN

Actualmente no existe discusión en que la transferencia de bienes y servicios a través de plataformas digitales cambió la forma de hacer negocios en el mundo; es más, la aparición misma de éstas ha permitido el surgimiento de formas y oportunidades de negocios que antes no se concebían.

La posibilidad de ofrecer bienes y servicios a través de internet se ha convertido para las empresas en una necesidad de mercado, pero también en una oportunidad para crecer y llegar a un número ilimitado de clientes. Aún las empresas que mantienen el tradicional sistema de ventas directas en grandes almacenes han entendido que para mantenerse vigentes deben ofrecer a sus clientes la posibilidad de realizar "compras digitales" y ofrecer sus servicios a través de plataformas digitales.

Esta nueva dinámica del comercio ha requerido que las empresas implementen aplicaciones virtuales que permitan a los usuarios acceder a una mayor oferta de bienes y servicios. Así, por ejemplo, la industria del turismo es uno de los sectores que mejor provecho ha sacado del internet, de tal manera que el antiguo sistema de hacer negocios por parte de las denominadas "agencias de viajes" se ha visto relegado por la aparición de páginas especializadas en venta de tiquetes, planes turísticos y oferta de hoteles, entre otros servicios que mueve esta industria, lo que le permite a los consumidores acceder a los servicios que más se ajusten a sus necesidades, gustos y capacidad económica. De igual manera, las más reconocidas marcas de vestuario, calzado, electrodomésticos, productos para el hogar, productos de belleza, mobiliario, artículos deportivos, así como la de los

prestadores de servicios de salud, transporte y alimentación, entre muchos otros sectores, han desarrollado sus propias Páginas Web para comercializar sus productos.

Gracias a esta oferta digital, los clientes sin desplazarse a ningún lugar y desde la comodidad de sus hogares u oficinas, pueden acceder desde sus PCs, Laptops o teléfonos celulares a las páginas de los fabricantes o comercializadores de bienes o de los prestadores de servicios para conocer sus productos, comparar precios y hacer la elección que más satisfaga sus necesidades.

Cuando luego de agotar este proceso se logra materializar una venta de un bien o un servicio a través de una plataforma digital, tal hecho queda necesariamente registrado en las bases de datos de las empresas, por muchas razones, entre ellas, para identificar al cliente, cantidad y calidad de bienes o servicios seleccionados, el lugar de entrega, la forma de pago, la emisión de la factura, la entrega de garantías, así como para fines internos como control de ventas e inventarios, control de despachos, control de cartera, fines tributarios, entre otros.

En la medida que este proceso de venta de bienes se repite se van generando, alimentando y consolidando las denominadas *bases de datos*, donde se recopila la información de los clientes. En los últimos tiempos la información que se puede extraer de estas bases de datos ha resultado muy valiosa para las empresas en la medida que les permite codificarla y analizarla para identificar preferencias de consumo de los distintos sectores de la población y así optimizar el direccionamiento de sus inversiones en temas de producción, comercialización, publicidad y mercadeo; en tal sentido las bases de datos se han convertido en un importante activo.

La custodia y manejo de las referidas bases de datos requiere de regulación legal en la medida que en ellas se maneja información reservada de personas naturales, que de ser expuesta abiertamente puede generar graves problemas a

los consumidores y, por ello, todas las empresas que manejen bases de datos deben necesariamente implementar políticas de manejo de datos que otorguen garantía de seguridad y confidencialidad a los clientes.

En este contexto este trabajo pretende describir el desarrollo la normativo de la protección de datos en Colombia como derecho derivado de protección a la intimidad y al buen nombre y también su comprensión desde la legislación Europea, quienes han considerado la protección de datos como un derecho autónomo[1] lo cual ha permitido un mejor desarrollo y libertad regulada para el intercambio de información valiosa a nivel comercial sin que ello se convierta en detrimento para los derechos fundamentales de las personas.

2. PLANTEAMIENTO DEL PROBLEMA

Aunque, como veremos más adelante, el desarrollo de normatividad en Colombia sobre la protección de datos es muy reciente, y salvo por la breve mención a la que hace referencia el lit. f del art. 50 de la Ley 1480 de 2011[2] sobre protección al consumidor en relación con la información, no han sido diseñadas particularmente ni se ha señalado de manera expresa que sean de aplicación en entornos digitales, sin embargo, es importante señalar que las mismas tienen aplicación en todos los medios a través de los cuales se suministre información o se realice inclusión, almacenamiento y tratamiento de datos de las personas, como por ejemplo cuando con el fin de intercambiar bienes o servicios éstos se requieren, y que como consecuencia, independientemente del medio a través del cual sean publicados o manipulados pueden constituir un riesgo para los derechos de las

[1] Determinando que el derecho a la protección de datos personales se ha conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;

[2] Articulo 50 Lit. f, Ley 1480 de 2011: Adoptar los mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos.

personas naturales así como lo expresa el Magistrado Eduardo Montealegre en las siguientes consideraciones *"a pesar de que las redes sociales digitales –generalistas o de ocio y profesionales- se consolidan como un espacio en el que se rigen normas similares a las del mundo no virtual, el acceso a las mismas acarrea la puesta en riesgo de derechos fundamentales, pues el hecho de que algunas de ellas se manejan a través de perfiles creados por los usuarios, por medio de los cuales se pueden hacer públicos datos e información personal, pueden traer como consecuencia la afectación de derechos como la intimidad, la protección de datos, la imagen, el honor y la honra"*[3]. Así pues y dado que hoy en día es común y necesaria la entrega de información personal a las empresas para adquirir bienes o servicios a través de plataformas virtuales, la cual genera, consolida y alimenta bases de datos, a su vez ésta dinámica impone a los empresarios responsabilidades para el manejo seguro y reservado de dicha información. En ese orden de ideas, se ha obligado a las empresas a otorgar a sus clientes o usuarios plena seguridad de reserva de la información que obtienen de éstos, la cual debe ser informada, limitada y consciente.

Por lo anterior el interrogante que se plantea respecto del particular es, cuál es el desarrollo en Colombia a la protección de datos personales y si las herramientas proporcionadas por nuestra legislación protegen los derechos constitucionales de las personas cuando otorgan consentimiento para su tratamiento especialmente al momento de adquirir bienes y servicios a través de plataformas digitales para lo cual se tomará como referencia también la normativa de la Unión Europea.

Para desarrollar éste interrogante en primer lugar es necesario recordar que en el desarrollo de sus actividades mercantiles los empresarios conforman bases de datos de sus clientes o usuarios, que les permiten identificar necesidades y gustos de los consumidores y de esa manera adoptar decisiones sobre producción y comercialización de bienes y servicios. Sin embargo, en los últimos años se ha demostrado que la protección de la información que suministran los usuarios y/o

[3] Corte Constitucional T-729/2002 M.P. Eduardo Montealegre

consumidores a las empresas que manejan sus bases de datos en plataformas digitales no es tan eficiente que permita garantizar que ésta no se pueda usar para fines distintos a los autorizados o que pueda terminar en manos terceros que la pueden utilizar con fines diversos, algunas veces ilegales o fraudulentos. La importancia del asunto planteado radica en que con las autorizaciones genéricas[4] los empresarios pueden estar vulnerando varias disposiciones constitucionales, entre ellas el derecho a la intimidad, consagrada en el artículo 15 o la responsabilidad del empresario a que se refiere el artículo 333. Por lo anterior, resulta de gran importancia que el Estado proteja a los consumidores que entregan su información personal y les otorgue facultades de decisión y autorregulación que les permita actuar de manera informada al momento de prestar su aceptación total o parcial al almacenamiento y uso posterior de sus datos.

Con el fin de desarrollar el problema planteado se toma como referencia la Constitución Política de Colombia y la regulación que traen las leyes 1266 de 2008 que regula la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países , la ley 1581 de 2012 en la cual se dictan disposiciones generales para la protección de datos personales, así como el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la ley 1581 de 2102, así como la incidencia de la Ley 1480 de 2011 sobre la protección al consumidor; igualmente se consultarán algunas sentencias de la Corte Constitucional, artículos de autores nacionales y extranjeros sobre el tema.

3. REGULACIÓN DEL TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA

[4] En lo que respecta al formato en que se presenta el contrato en la pantalla del usuario, por lo general este trae aparejadas serias dificultades que obstan a su validez (v. gr., el texto del contrato suele aparecer en idioma extranjero o con deficiencias en la traducción que lo hacen inentendible; se requiere que el usuario acepte las condiciones generales antes de utilizar el producto, pero después de haberlo adquirido, incluso cuando el usuario no pudo tener acceso a ellas para leerlas; al pie de dichos contratos, se estila colocar la leyenda “Acepto”, “Estoy de acuerdo” u otra similar, marcada por defecto, sin requerir acción alguna del usuario, entre otras).

A continuación, se expondrán algunas consideraciones sobre la protección de datos en Colombia y su uso en las plataformas digitales:

Como se ha expresado en el capítulo introductorio las necesidades actuales de los consumidores y el libre acceso a productos y servicios a través de las plataformas electrónicas ha impulsado el uso de los datos personales como si se tratara de un "bien" más en el mercado. Sin embargo, Colombia legislativa y jurisprudencialmente[5] ha desarrollado mecanismos con el fin de proteger, en todos los campos, el derecho establecido en el artículo 15 de la Constitución que consagra lo siguiente: *"todas las personas…tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".* Lo anterior quiere decir que en Colombia el derecho al Habeas Data[6] es un derecho de categoría constitucional, al igual que ocurre en la Unión Europea y no es un derecho relacionado únicamente con las leyes de protección al consumidor como si ocurre en Norteamérica y por lo cual reviste un significado diferente en su ámbito de aplicación.

Para la ley 1266 de 2008, en desarrollo de los derechos y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a los que se refiere el artículo 15 de la Constitución Política y *"cuyo ámbito de aplicación es tanto para las entidades públicas y privadas, salvo las que entidades que por motivos de orden y/o seguridad pública o para efectos estadísticos se refiera"*[7]*,* la protección de datos personales tiene un amplio margen de acción en todas las esferas del desarrollo social y económico del país y con mayor frecuencia, hoy en día, en las relaciones entre las personas a través de las redes sociales o plataformas digitales a las que se accede a infinitos bienes y

[5] T-414-02/SU-082-95/T-097-95/T-119-95/T-309-99/C-1011-2008/C-748-2011

[6] A juicio de la Corte está integrada 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 uso y circulación, de conformidad con las regulaciones legales.

[7] Articulo 2

servicios. Por lo anterior es necesario e imprescindible que dichas políticas de protección sean aplicables en todos los ámbitos del comercio, incluso el electrónico.

Sin embargo, la ley 1266 de 2008 tiene un alcance restringido, principalmente a las bases de datos personales, y especialmente a la financiera, crediticia, comercial y de servicios, así como de la proveniente de terceros países, lo que implica que no tenía un alcance general para todos los tipos de datos personales y/o bases de datos que los contengan. La necesidad en su momento surgió de las múltiples denuncias que realizaron, incluso a través de recursos judiciales como la acción de tutela, algunas de ellas a las que se hace referencia anteriormente, y que tuvieron su mayor momento de eclosión con las plataformas como Datacrédito dado que los datos sensibles de las personas quedaban expuestos y podían ser revisados y utilizados por terceras personas sin interés en dicha información y que su conocimiento afectaba gravemente su derecho a la intimidad, buen nombre y derechos conexos al habeas data.

La mencionada ley con el fin de identificar los datos a los que hace referencia ha diferenciado los tipos de datos personales dependiendo del nivel de riesgo que pueda comprometer los derechos de sus titulares, los cuales pueden ser: *públicos,* siendo aquellos los que *no requieren autorización* para su tratamiento como por ejemplo el nombre o el estado civil, *semiprivados y privados* como aquellos que *requieren consentimiento previo y expreso de su titular* (art. 6-1. Parágrafo), salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países frente a los cuales se requiere un manejo diferente por su clase de protección e impacto que puede tener frente a los derechos de las personas.

Así mismo ha definido a los tipos de personas que intervienen en la recolección y manejo de dichos datos de la siguiente manera: *titular de la información*, como aquella persona natural o jurídica a la que se refiere la información; *fuente de información* como aquella que recibe la información para su tratamiento; *operador*

de información como aquel destinatario que tiene calidad de usuario y fuente; y por último, el *usuario* que es toda persona que tiene acceso a la información.

Para cada una de las categorías antes mencionadas se señalan deberes de conservación y divulgación, especialmente por parte de las fuentes y los operadores que son quienes habitualmente utilizan la información, entre los que se destacan los siguientes: "*garantizar en todo tiempo al titular el pleno y efectivo derecho de habeas data y de petición, permitir el acceso únicamente a las personas que de conformidad con lo previsto en esta ley pueden tener acceso a ella, adoptar un manual interno de políticas y procedimientos para garantizar el efectivo cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos por parte de los titulares, conservar con las debidas seguridades los registros almacenados para impedir su deterioro, perdida, alteración, uso no autorizado o fraudulento".*[8]

Posteriormente, en la ley 1581 de 2013, la cual, a diferencia de la anterior, tiene un alcance mayor en la medida que su ámbito de aplicación es para todas las bases de datos como se expresa en su articulo No. 2 así: *"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada".* Por lo anterior, complementa y precisa lo señalado en la ley 1266 de 2008 cuando se refiere a los principios rectores aludiendo a que *"el tratamiento 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 releve el consentimiento"*[9] y seguidamente señala unas categorías especiales de datos o datos sensibles describiéndolos 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*

[8] Artículo 7
[9] Artículo 4

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"[10] sobre los cuales se prohíbe su tratamiento salvo cuando *"el titular haya dado su autorización explícita".* Lo anterior para llamar la atención en que, incluso tratándose de datos denominados sensibles, el titular puede otorgar su consentimiento para el tratamiento de su información; sin embargo, esto ninguna dificultad revestiría si las personas al otorgar su consentimiento lo realizaran de manera libre e informada, quiere decir, que las autorizaciones físicas o digitales que les son suministradas por los operadores o fuentes tuvieran la salvedad o fueran lo suficientemente discriminadas en su formato que le permitieran al titular reservarse su derecho legítimo a entregar una u otra información. La práctica nos indica que dichos formatos suelen ser genéricos y de respuestas Si o No, lo cual no permite margen de discrecionalidad a lo permitido. Al respecto, la ley se queda corta al señalar en su artículo 11 que *"la información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos"* y en pocos casos se atiende al literal b del artículo 12 de la misma norma *"El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes".* Sobre este punto la Corte Constitucional señala *"que los riesgos para los derechos fundamentales en redes sociales pueden generarse por tres situaciones: la falta de conciencia de los usuarios sobre el hecho de que sus datos personales son accesibles por cualquier persona y que éstos pueden tener un gran valor en el mercado; los datos personales pueden ser utilizados por otros usuarios de forma ilícita y malintencionada y es posible que se publique en la red información falsa o sin autorización del usuario"*[11]

Ahora bien, la expedición del Decreto 1377 de 2013 incluye otros conceptos de vital importancia en el mundo de los datos electrónicos como la inclusión del Aviso

[10] Artículo 5
[11] Corte Constitucional T-729/2002 M.P. Eduardo Montealegre

de Privacidad *"mediante el cual se informa acerca de la existencia de políticas de tratamiento de la información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales"*[12] y que se refuerza más adelante en la misma norma cuando se señala el contenido del aviso de privacidad en cuanto a la necesidad y obligatoriedad de informar sobre el tratamiento al cual serán sometidos los datos y su finalidad así como *el carácter facultativo cuando se trate de datos sensibles*[13], precepto que salvo por los datos públicos, deberían estar individualizados en el consentimiento o autorización que se solicita al titular.

Por último, es de tal importancia el manejo de la información y la transferencia de la misma que Colombia, a través de la Delegatura para la Protección de Datos de la Superintendencia de Industria y Comercio, la cual ejerce funciones de Control y Sancionatorios en asuntos relacionados con la Protección de la Información, pertenece a la Red Iberolatinoamericana de Protección de Datos (RIPD) y de la cual hacen parte 24 países de la región y que desde hace algunos años se han dedicado a redactar y publicar Estándares para la Protección de Datos cuyos objetivos son los siguientes:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.
- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.
- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.

[12] Artículo 1
[13] Artículo 15

- Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

Si bien es cierto que la organización pretende homogenizar las políticas de protección de datos en los países miembros se hace evidente que su objetivo principal es a través de dichas políticas se permita de manera más segura la transferencia de datos con fines comerciales y facilitar así el comercio electrónico.

4. LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA

Frente al desarrollo internacional en el marco del comercio digital y la protección de datos, especialmente la normativa de la Unión Europea ha desarrollado lo siguiente:

Su marco normativo inicia en la Constitución española de 1978 en la cual se lee lo siguiente: *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*[14]*,* quiere decir que, incluso antes del auge de las plataformas digitales y previendo el impacto de éstas en la vida de las personas, legislaciones como por ejemplo la Europea ya daba cuenta de los riesgos que implicaría la obtención y tratamiento de datos a través de medios masivos de difusión de información. Así es como en desarrollo de los derechos como la intimidad, a la protección y procesamiento de datos se le ha dado un mayor alcance calificándolo como un derecho autónomo, protegiendo incluso la totalidad de los datos de carácter personal y no solo aquellos que se clasifican como íntimos.

Para la normatividad europea, como se mencionó anteriormente, la protección de datos dista de ser una concepción meramente de derecho de consumo para

[14] Artículo 18.4 CE

convertirse en un derecho fundamental principal, de allí deriva su importancia en otros ámbitos como el comercio, ya que a través de la protección al individuo se genera también confianza entre las empresas y los consumidores de bienes y servicios lo que a su vez genera mayor competitividad y transparencia en los procesos de intercambio. Lo anterior para afirmar que proteger a la persona en estos casos resulta un medio efectivo para la libre circulación de los datos a través de diversos medios con el fin de lograr los objetivos en un mercado globalizado.

Como primer antecedente de regulación legal, la Directiva 95/46/CE nace de la necesidad de permitir el flujo de datos personales de manera más segura y libre entre los Estados Miembros de la Unión Europea como se describe en su artículo 1 de la siguiente manera: *"Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales" y " Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1".*

En cuanto a su ámbito de aplicación es aún más específica en el sentido de que incluye de manera expresa su aplicación en los entornos digitales y a su tratamiento "automatizado"[15]. Así mismo excluye de su ámbito de aplicación algunas actividades como *"el tratamiento de datos que tenga como objeto la seguridad pública, la defensa, la seguridad del Estado, y las actividades del Estado en materia penal, las actividades exclusivamente personales o domésticas"*[16]

Los principios generales para el tratamiento de datos personales son principalmente la calidad y la legitimación para acceder a los mismos; por calidad se refiere a que los datos sean recogidos con fines determinados, explícitos, adecuados, pertinentes y no excesivos en relación a los fines con los que se

[15] D 95/46/CE Artículo 3 apartado 1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
[16] D 95/46 CE Artículo 2.

recaben; exactos, y en lo posible, actualizados; en cuanto a esto último la norma prevé que en caso de que los datos sean inexactos o incompletos sean suprimidos o rectificados. Adicionalmente adecua el criterio de necesidad en el sentido de que los mismos no pueden ser conservados por un periodo indefinido de tiempo sino únicamente durante el tiempo para cuyo fin fueron recolectados. Frente al principio de legitimación, solo podrán ser tratados los datos cuando el interesado ha dado su consentimiento de forma inequívoca, además se destaca su utilización cuando sea necesaria para la ejecución de un contrato en el que el interesado sea parte.

Por otra parte, existen también algunas prohibiciones para el tratamiento de los datos cuando éstos revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los relativos a la salud o la sexualidad. (CE 95/46).

Posteriormente, el Parlamento Europeo en el año 2016 se expide el Reglamento UE 2016/679 (Reglamento General de Protección de Datos) con el fin de dar un contexto más homogéneo en la aplicación y el nivel de protección adecuado a las personas físicas en la transferencia de datos dentro de la Unión y con terceros países. Sin embargo, a la misma vez este Reglamento incentiva aún más la libre circulación de los datos y lo describe como un derecho autónomo[17] en lo cual la Directiva del año 1995 no resultaba tan específica.

Por otro lado, el Reglamento es más incluyente de la economía y proporciona seguridad jurídica y transparencia a los operadores económicos como las microempresas y las pequeñas y medianas empresas flexibilizando los registros[18], también, en el entendido que solo es aplicable a las personas físicas (no jurídicas)[19]

[17](1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.

[18] (13) Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados.

[19] (14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

En cuanto a su ámbito territorial de aplicación se extiende la protección a todas las personas independientemente de su nacionalidad o lugar de residencia lo que permite que, tratándose de datos, éstos se encuentren protegidos si el responsable de los mismos tiene su lugar de recolección o de almacenamiento en alguno de los estados de la Unión, así su tratamiento no se de en su territorio. Cuando los interesados residan en la Unión, pero el responsable o el encargado no, el Reglamento se aplica cuando esté relacionado con*: "a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a éstos se les requiere su pago, o b) el control de su comportamiento en la medida que éste tenga lugar en la Unión"*[20].

Amplía el concepto de tratamiento de datos a la *"recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"* de los mismos, a diferencia de la Directiva anterior que limitaba el concepto a algunos de éstos tratamientos.

La norma agrega como principio la transparencia en el trato de datos personales, Sobre este principio dedica la sección 1 del Capítulo III "derechos del interesado" en cuanto a que la disponibilidad de los datos para el interesado debe ser concisa, inteligible y de fácil acceso y para su obtención debe entregarse por parte del responsable del tratamiento por lo menos la siguiente información: *a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f)*[21], *los intereses legítimos del responsable o de un tercero; e) los destinatarios o las*

[20] CE Artículo 3 (2) Reglamento (UE) 2016/679 el 27 de abril de 2016

[21] 1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional…"[22]

Adicionalmente para garantizar un tratamiento de datos leal y transparente se debe permitir al interesado conocer información sobre el plazo[23], la existencia del derecho de rectificación y supresión así como de limitación u oposición al tratamiento, el derecho a la portabilidad de los mismos, y cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a),[24] o el artículo 9, apartado 2, letra a)[25], la existencia del derecho a retirar el consentimiento en cualquier momento, el derecho de reclamación ante la autoridad de control y si se trata de un requisito necesario para suscribir un contrato informar de las posibles consecuencias de no facilitar tales datos. [26]

Cuando los datos no hayan sido obtenidos directamente del interesado como puede ocurrir por ejemplo en su extracción de fuentes de acceso público (páginas de internet) y éstos vayan a ser tratados será necesario informar al interesado sobre su tratamiento y si es del caso solicitar su autorización para dicho tratamiento. Para ello el responsable del tratamiento facilitará la información indicada en los párrafos anteriores *a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos; b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.*

---

[22] Artículo 6 Reglamento (UE) 2016/679 el 27 de abril de 2016

[23] Ya que, de no existir, la información negativa mantenida en bases de datos de manera indefinida podría llegar a causar graves perjuicios para las personas y sus familiares

[24] 1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

[25] …a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados…

[26] Artículo 13 Reglamento (UE) 2016/679 el 27 de abril de 2016

5. CONCLUSIONES

Una vez descritas las principales herramientas normativas con las que cuenta la legislación colombiana hoy en día para el tratamiento de datos personales e ilustrando como se ha desarrollado a través de la jurisprudencia este importante derecho de las personas, se puede concluir que desde la vigencia de la Constitución Política de 1991, esta materia ha tenido un importante avance y además es equiparable con las necesidades del comercio; pero que, al igual que ocurre en otras legislaciones del mundo, como por ejemplo la de los países europeos es un proceso susceptible de mayores previsiones y regulaciones, en la medida que las necesidades digitales que cada vez se manifiestan más rápidamente creen la necesidad de definir políticas más eficaces para la protección de las personas a través de sus datos.

Por otro lado, también es notorio que los estándares de protección de la Unión Europea son más amplios y tienen en cuenta mayor cantidad de eventos que pueden darse en el contexto del tratamiento de los datos, de ésta manera promueven un mayor alcance territorial y extraterritorial de sus normas con miras a proteger a sus ciudadanos normatividad que podría ser un ejemplo a seguir para nuestras futuras legislaciones.

Por último, es importante destacar los avances que Colombia ha tenido en ésta materia en un tiempo menor de desarrollo del que han tenido otros países y como se ha adecuado a las necesidades del mercado y sigue trabajando en el acercamiento cada vez mayor a los estándares internacionales en la materia, lo que sin duda le permitirá alcanzar mejores objetivos en el mundo de comercio electrónico protegiendo a sus ciudadanos de las amenazas a las que

indiscutiblemente se someten las personas al ingresar a entornos digitales en los cuales no exista una debida protección de su información.

6. BIBLIOGRAFÍA

- Constitución Política de Colombia
- Constitución Española de 1978
- Ley 1266 de 2008
- Ley 1581 de 2013
- Ley 1480 de 2011
- Decreto 1377 de 2013
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Corte Constitucional de Colombia. (1992). Sentencia T-414. M.P.: Ciro Angarita Barón.
- Corte Constitucional de Colombia. (1995). Sentencia SU-082. M.P.: Jorge Arango Medina.
- Corte Constitucional de Colombia. (1995). Sentencia T-097. M.P.: José G. Hernández Galindo.
- Corte Constitucional de Colombia. (1995). Sentencia T-119. M.P.: José G. Hernández Galindo.
- Corte Constitucional de Colombia. (1999). Sentencia T-309. M.P.: Alfredo Beltrán Sierra.
- Corte Constitucional de Colombia. (2002). Sentencia T-792. M.P.: Eduardo Montealegre Lynett.
- Corte Constitucional de Colombia. (2008). Sentencia C-1011. M.P: Jaime Córdoba Triviño.

- Corte Constitucional de Colombia. (2011). Sentencia C-748. M.P: Jorge Pretelt Chaljub.
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos, Red Iberoamericana de Protección de Datos Personales, 20 de junio de 2017
- Monsalve, V. (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, 20, 39, 163-195. DOI: http://dx.doi.org/10.18359/prole.2729
- El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea.
  By: Reigada, Antonio Troncoso. *Revista de Derecho Comunicaciones y Nuevas Tecnologías.* dic2012, Issue 9, preceding p5-38. 38p. Language: Spanish. , Base de datos: Fuente Académica Premier.
- El derecho al olvido: análisis comparativo de las fuentes internacionales con la regulación colombiana. The right to be forgotten: a comparative analysis of international sources with colombian regulations. / O direito ao esquecimento: análise comparativo das fontes internacionais com a regulação colombiana. By: Manrique Gómez, Valentina. *Revista de Derecho Comunicaciones y Nuevas Tecnologías.* jul-dic2015, Issue 14, p1-25. 25p. 1 Color Photograph, 1 Graph. Language: Spanish. DOI: 10.15425/redecom.14.2015.09. , Base de datos: Fuente Académica Premier.
- Derecho a la privacidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales. Buenos Aires, jueves 9 de junio de 2016 • ISSN 1666-8987 • Nº 13.974 • AÑO LIV • ED 268.

CARTA DE AUTORIZACIÓN DE LOS AUTORES
(Licencia de uso)

Bogotá, D.C., 4 de febrero de 2020

Señores
Biblioteca Alfonso Borrero Cabal S.J.
Pontificia Universidad Javeriana
Cuidad

Los suscritos:

Laura Carolina Mantilla de Valera	, con C.C. No	53053583
	, con C.C. No	
	, con C.C. No	
	, con C.C. No	
	, con C.C. No	
	, con C.C. No	

En mi (nuestra) calidad de autor (es) exclusivo (s) de la obra titulada:
TRATAMIENTO DE DATOS PERSONALES Y LAS PLATAFORMAS DIGITALES RESEÑA SOBRE COLOMBIA Y LA UNIÓN EUROPEA

(Por favor señale con una "x" la opción que aplique)

Tesis Doctoral ○
Tesis de Maestría ○
Trabajo de Grado Especialización ◉
Trabajo de Grado Pregrado ○
Otro ○

Cual: Especialización en Derecho Comercial

Premio o distinción SI ○ NO ◉

Cual: _____

Año de Presentación: 2020

Por medio del presente escrito autorizo **(autorizamos)** a la Pontificia Universidad Javeriana para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mi (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autorizan a la Pontificia Universidad Javeriana, a los usuarios de la Biblioteca Alfonso Borrero Cabal S.J., así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado un convenio.

Información de confidencialidad:

Este documento contiene información privilegiada, estratégica, secreta, confidencial o similar, o hace parte de una investigación que se adelanta y cuyos resultados finales no se han publicado.

SI ◯ NO ◉

Si su respuesta es **SI** por favor indique a continuación el motivo y el tiempo de restricción.

Motivo de restricción:
Tiempo de restricción

Nota: *El documento quedara restringido para la consulta por el tiempo de embargo indicado, o indefinidamente en caso de que éste no se registre, una vez concluido dicho periodo (si aplica), indicar a continuación el tipo de consulta que se autoriza.*

Marque a continuación con una **X** el tipo de consulta que autoriza.

AUTORIZO (AUTORIZAMOS)	SI	NO
1. La consulta electrónica a través del catálogo Biblos y el Repositorio Institucional, así como la inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previo convenio perfeccionado con la Pontificia Universidad Javeriana para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones.	x	

Aceptamos los términos de la licencia Creative Commons de Reconocimiento-No comercial-Sin obras derivadas 2.5 Colombia.

Para más información consulte:
http://creativecommons.org/licenses/by-nc-nd/2.5/co/

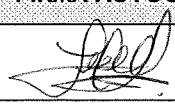
De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

De manera complementaria, garantizo (garantizamos) en mi (nuestra) calidad de estudiante (s) y por ende autor (es) exclusivo (s), que la Tesis o Trabajo de Grado en cuestión, es producto de mi (nuestra) plena autoría, de mi (nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy (somos) el (los) único (s) titular (es) de la

misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Pontifica Universidad Javeriana por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o restricción alguna, puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, *"Los derechos morales sobre el trabajo son propiedad de los autores"*, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Pontificia Universidad Javeriana está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

NOMBRE COMPLETO	No. del documento de identidad	FIRMA AUTÓGRAFA
Laura Carolina Martillo de Valera	53053583	

FACULTAD Ciencias Jurídicas

PROGRAMA ACADÉMICO Especialización en Derecho Comercial