LUZ MÓNICA HERRERA ZAPATA
JORGE MURGUEITIO CABRERA
SANDRA MILENA ORTIZ LAVERDE
Coordinadores

II

Ecosistema digital en sus distintos desarrollos y las tecnologías disruptivas

Las TIC y la SOCIEDAD DIGITAL

Doce años después de la ley

ÉDGAR GONZÁLEZ LÓPEZ / Director

CONSEJO DE ESTADO
JUSTICIA - GUÍA - CONTROL

Universidad Externado de Colombia

ÉDGAR GONZÁLEZ LÓPEZ
(DIRECTOR)

LUZ MÓNICA HERRERA ZAPATA
JORGE MURGUEITIO CABRERA
SANDRA MILENA ORTIZ LAVERDE
(COORDINADORES)

LAS TIC Y LA SOCIEDAD DIGITAL

DOCE AÑOS DESPUÉS DE LA LEY

TOMO II
ECOSISTEMA DIGITAL EN SUS DISTINTOS DESARROLLOS Y LAS TECNOLOGÍAS DISRUPTIVAS

UNIVERSIDAD EXTERNADO DE COLOMBIA

Las TIC y la sociedad digital [e-book] : doce años después de la ley. Tomo II, ecosistema digital en sus distintos desarrollos y las tecnologías disruptivas / Édgar González López (director) ; Luz Mónica Herrera Zapata, Jorge Murgueitio Cabrera, Sandra Milena Ortiz Laverde (coordinadores) ; presentación Hernando Parra Nieto ; Germán Darío Arias Pimienta [y otros]. -- Bogotá : Universidad Externado de Colombia. 2021.

1 recurso electrónico (874 páginas) : gráficos ; 24 cm.

Incluye referencias bibliográficas al final de cada capítulo.

ISBN: 9789587908285 (e-book)

1. Tecnologías de la información y la comunicación – Legislación – Colombia 2. Tecnologías de la información y la comunicación -- Innovaciones tecnológicas – Colombia 3. Sociedad de la información -- Aspectos jurídicos – Colombia 4. Competencia (Derecho) – Colombia 5. Big data -- Colombia I. González López, Édgar, director II. Herrera Zapata, Luz Mónica, coordinadora III. Murgueitio Cabrera, Jorge, coordinador IV. Ortiz Laverde, Sandra, coordinadora V. Parra Nieto, Hernando, presentación VI. Universidad Externado de Colombia VII. Título

LE303.4833 SCDD 21

Catalogación en la fuente -- Universidad Externado de Colombia. Biblioteca.

noviembre de 2021

ISBN 978-958-790-727-8
e-ISBN 978-958-790-728-5

Calle 12 n.º 1-17 este, Bogotá
Teléfono (601) 342 0288
publicaciones@uexternado.edu.co
www.uexternado.edu.co

Primera edición: noviembre de 2021

Corrección de estilo: José Curcio Penen
Diseño de cubierta: Departamento de Publicaciones
Composición: María Libia Rubiano
Impresión y encuadernación: Xpress Estudio Gráfico y Digital S.A.S. - Xpress Kimpres
Tiraje: de 1 a 1.000 ejemplares

Impreso en Colombia
Printed in Colombia

CAPÍTULO 17

Protección de datos para el sector TIC: las tendencias en su regulación y su estado en Colombia

ANDRÉS FERNÁNDEZ DE CASTRO MUÑOZ*

SUMARIO

RESUMEN

El contexto del sector de las TIC en el cual se discutió y aprobó la Ley 1581 ciertamente es diferente al actual. A pesar de haberse presentado iniciativas tendientes a realizar algunas actualizaciones a la normatividad en materia de protección de datos en Colombia, ellas no se han elevado al rango de ley, por lo que aún existen incertidumbres en lo relativo a ciertos aspectos de la aplicación de la ley colombiana. Adicionalmente, con posterioridad a la Ley 1581 se observan tendencias regulatorias diferentes a la aproximación actual de protección de datos contenida en la norma colombiana, por ejemplo, en materia de servicios y nuevas funcionalidades que se soportan en

---

* LL.M en Media Law con énfasis en Telecomunicaciones, Medios, Protección de Datos y Seguridad de la Información del Queen Mary University of London. Asociado senior del grupo de práctica de Tecnología, Comunicaciones y Protección de Datos en Gómez-Pinzón Abogados. Correo-e: afernandezdecastro@gomezpinzon.com.

comunicaciones electrónicas. La modernización parcial del sector a través de las Leyes 1978 y 2108 puede servir de excusa para enfocarse ahora en otros aspectos normativos en los que se requiere certeza, como el alcance de las obligaciones en materia de protección de datos personales. Por lo anterior, a través del presente capítulo se estudia el estado actual del régimen aplicable al sector TIC en Colombia *versus* otros cuerpos normativos más recientes, con el fin de identificar si existen elementos de juicio que ameriten su revisión y actualización, o si las condiciones vigentes son suficientes para las necesidades de los distintos actores.

PALABRAS CLAVE

Protección de datos, privacidad en Internet, Ley 1581 de 2012, Ley 1341 de 2009, contratación electrónica, comunicaciones electrónicas.

INTRODUCCIÓN

La importancia del uso de datos para el sector de las Tecnologías de la Información y las Comunicaciones (TIC) es innegable. No sería posible concebir la operación de un Proveedor de Redes y Servicios de Telecomunicaciones (PRST) o el funcionamiento de una plataforma de comercio electrónico o de una red social, sin que los respectivos prestadores procesen información de los terceros que interactúan con ellos, incluyendo un alto volumen de datos personales.

Incluso los gobiernos han evidenciado que las TIC son un gran dinamizador de la economía, y que la utilización de grandes volúmenes de información es también un insumo para el diseño y la implementación de políticas públicas. En Colombia, a través del Documento Conpes 3920, también conocido como Política Nacional de Explotación de Datos (*big data*) (DNP, 2018), se reconoció que el aprovechamiento de los datos permite, entre otros, generar información y conocimiento para la posterior creación y mejora de los procesos, productos y servicios, solucionar problemas de política pública, empresariales e incluso académicos, y facilitar la innovación al ser mediado por analítica.

La emergencia sanitaria ocasionada por el Covid-19 en el año 2020 y la implementación de medidas de aislamiento social generaron de manera inusitada un incremento en la dependencia de los ciudadanos de soluciones

no tradicionales para acceder a bienes y servicios, y en especial, un aumento en el uso de las tecnologías en actividades cada vez más cotidianas.

Dentro de las distintas categorías de información que son objeto de procesamiento por los agentes del sector TIC, los datos personales y las obligaciones de los sujetos a cargo de su protección merecen especial atención. Ciertamente se ha recorrido un largo camino desde 1948 cuando en la Declaración Universal de Derechos Humanos se formuló una primera protección contra injerencias arbitrarias en la vida privada y la correspondencia, así como contra ataques a la honra o a su reputación. Actualmente está identificado incluso el carácter autónomo de la intimidad y la protección de los datos personales, lo que fue ratificado por la Corte Constitucional en la sentencia de control constitucional al Proyecto de Ley que antecedió a la Ley Estatutaria 1581 de 2012 (Ley 1581)[1], en la que resaltó la importancia del segundo de ellos en una sociedad globalizada donde la circulación de información es permanente. Aun cuando para la Corte Constitucional existe una estrecha relación entre ambos derechos, el derecho de autodeterminación informativa implica unas garantías diferenciables cuya protección podrá ser perseguida por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige con respecto a su procedencia. No obstante reconocer la autonomía de ambos derechos, y dado que el régimen legal que será objeto de análisis se refiere a ambos, para efectos de este capítulo se utilizarán las expresiones derecho a la privacidad o al *habeas data* o a la protección de datos para referirlos, salvo que por una circunstancia concreta se deba hacer la distinción.

En materia de protección de datos, además del marco dictado por la Ley 1266 de 2008 relativo a la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países, se cuenta con la Ley 1581, mediante la cual se dictaron disposiciones generales para la protección de los datos personales, y sus normas reglamentarias. Por su parte, el marco legal del sector TIC está dado por la Ley 1341 de 2009, el cual, no obstante ser anterior a la Ley 1581, reconoce al *habeas data*[2] como un principio orientador de la protección de los derechos de los usuarios.

Coincidiendo con los diez años de expedición de la Ley 1341, se expidió la Ley 1978 de 2019, por la cual se pretendió modernizar la regulación del

---

1 Corte Constitucional. Sentencia C-748 de 2011. Bogotá, 6 de octubre de 2011, M. P.: Jorge Pretelt Chaljub.

2 Artículo 2.º de la Ley 1341.

sector TIC, sin que se incluyera regulación alguna sobre el derecho fundamental del artículo 15 de la CPC. Situación similar ocurrió con la expedición de la Ley 2108 de 2021. Sin embargo, a casi diez años de su vigencia, no se ha realizado ninguna reforma a la Ley 1581 de 2012 que tienda a revisar las condiciones vigentes del régimen de protección de datos personales.

El contexto histórico del sector de las TIC para los momentos de discusión y expedición de las Leyes 1341 de 2009 y 1581 de 2012 dista del actual, y a nivel global se observa la implementación de marcos regulatorios en términos de protección de datos personales que incluyen componentes novedosos respecto de las condiciones previstas en la legislación colombiana. Una de las normas que sirvió de inspiración para la Ley 1581 de 2012, la Directiva 95/46/CE del Parlamento Europeo y del Consejo[3], fue derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea (Reglamento General de Protección de Datos de la Unión Europea o RGPD). Por su parte, se expidió la Ley de Privacidad del Consumidor de California (CCPA, por sus siglas en inglés) que del mismo modo que el RGPD, regula situaciones que vale la pena considerar. Del mismo modo, la legislación europea incluye una Directiva específica sobre la privacidad y las comunicaciones electrónicas[4], sobre la cual se presentó una propuesta de reforma para adaptarse a la realidad actual del sector y con ello "aumentar la seguridad de los servicios digitales y la confianza que los ciudadanos depositan en ellos"[5].

Dada la intrínseca relación entre el sector TIC y el procesamiento de datos personales, en el presente capítulo se identifican algunas tendencias regulatorias diferentes al modelo colombiano, de manera que se pueda concluir si existen elementos de juicio que ameriten la revisión de las condiciones actuales, en particular, con miras a ofrecer mayor certeza jurídica a un sector cada vez más relevante, y sin que ello implique bajo ninguna circunstancia el desmedro de la protección de los derechos de los ciudadanos.

---

3 Numeral 2.1.4. del Conpes 3920.

4 Directiva 2002/58/CE del Parlamento Europeo y el Consejo de la Unión Europea.

5 Exposición de Motivos de la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas.

1. EL RÉGIMEN LEGAL APLICABLE EN COLOMBIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES AL SECTOR TIC

1.1. EL USUARIO COMO TITULAR DE DATOS PERSONALES Y OTROS CONCEPTOS RELEVANTES

Este capítulo toma como contexto normativo el régimen aplicable en materia de protección de datos, así como las vicisitudes de los agentes del sector TIC, entendidos como los actores que participan de las industrias manufactureras, comerciales y de servicios, es decir, quienes recogen, procesan, crean, transmiten o muestran datos e información electrónicamente[6]. La descripción anterior, que años atrás podía incluir solamente a los PRST, hoy en día comprende un abanico de empresas (incluso algunas originalmente del sector real) que procesan datos e información electrónicamente sin necesidad de contar con una red propia, sino a través de la utilización de servicios de telecomunicaciones prestados por terceras partes.

El marco constitucional en materia de protección de datos dado por el artículo 15 de la CPC permitió desarrollar las Leyes 1266 y 1581, así como sus decretos reglamentarios y múltiples decisiones e instrucciones administrativas y judiciales. El origen de la Ley 1581 se debió a la insuficiente protección que otorgaba la Ley 1266, pues el alcance de esta última es sectorial, enfocado en el procesamiento de información necesaria para determinar el riesgo crediticio de una persona, y no incluye información diferente a la financiera, crediticia, comercial, de servicios y la proveniente de terceros países (Remolina Angarita, 2013). El análisis de este capítulo considera cada una de ellas en cuanto corresponda, pero reconociendo que los conceptos generales que se utilizan, en línea con legislaciones extranjeras, son los referidos en la Ley 1581.

Por su parte, no obstante ser anterior a la Ley 1581, la Ley 1341 incluye algunas disposiciones que, aunque tímidas (quizá por su naturaleza de ley ordinaria), son relevantes para el sector, en particular por su énfasis en la figura del usuario[7]. La ley es clara en disponer que el cumplimiento de los

---

6 Artículo 9.º de la Ley 1341.

7 "Persona natural o jurídica consumidora de servicios de comunicaciones" según la Resolución 5050 de 2016 de la CRC.

deberes derivados del *habeas data* asociados con la prestación del servicio es uno de los principios orientadores del sector[8], lo cual se ratifica con el derecho que todos los usuarios tienen de recibir protección en cuanto a su información personal, así como a que se les garanticen la inviolabilidad y el secreto de las comunicaciones, y la protección a la publicidad indebida, según la CPC y la ley. Para tales efectos, en lo que resulte aplicable, la Ley 1341 prevé la competencia de la Comisión de Regulación de Comunicaciones (CRC) para regular el régimen jurídico de protección al usuario.

Al extrapolar el concepto de usuario como destinatario de la protección de la Ley 1341 a las disposiciones y definiciones en materia de protección de datos personales de la Ley 1581[9], necesariamente se debe hacer referencia al *titular*, es decir, a la persona natural cuyos datos personales sean objeto de tratamiento. No obstante que la definición de usuario utilizada por la CRC incluye a las personas jurídicas, la protección de la Ley 1581 solamente se extiende a personas naturales. Por *datos personales* se hace referencia a cualquier información vinculada o que pueda asociarse a uno o varios titulares determinados o determinables; mientras que por *datos sensibles* se entienden aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación[10]. El *tratamiento* es cualquier operación sobre datos personales, y puede ser realizado por el *responsable*, es decir, aquella persona que por sí misma, o en asocio con otras, decide sobre el tratamiento de los datos personales, o por el *encargado*, es decir, aquella persona que por sí misma o en asocio con otras, realiza el tratamiento de los datos personales por cuenta de un responsable. Adicionalmente existen dos figuras legales en materia de circulación de los datos personales: la *transferencia* y la *transmisión*; la primera tiene lugar cuando un responsable, directamente o a través de un encargado, envía los datos personales a un receptor, que a su vez será responsable, mientras que la segunda se refiere a la comunicación

---

8 Artículo 2.º de la Ley 1341.

9 Las palabras en letra itálica en este párrafo corresponden a las definiciones de la Ley 1581 y el Decreto 1377 de 2013, compilado en el capítulo 25 del Decreto 1074 de 2015.

10 Como, por ejemplo, según el artículo 5.º de la Ley 1581, "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

de los datos personales para que un encargado los trate por cuenta y para los fines del responsable.

En materia de protección de datos personales, los responsables y los encargados son quienes asumen la mayor carga regulatoria en lo que concierne a la protección de los derechos de los titulares durante el tratamiento; sin embargo, ello no obsta para que los titulares también asuman un manejo responsable en la materia, evitando difundir públicamente información personal a través de herramientas que permitan a terceros un acceso masivo e indiscriminado.

Aun cuando no es objeto del presente capítulo, se debe mencionar que a través de la Ley 1273 de 2009 se incorporó al ordenamiento penal la protección de la información y de los datos como bien jurídico tutelado, e incluso se dispusieron dos tipos penales específicos: la violación de datos personales y la suplantación de sitios web para capturar datos personales.

1.2. La reglamentación específica y su aplicación al sector TIC

Para facilitar la aplicación de la Ley 1581 el Gobierno expidió el Decreto 1377 de 2013, en el cual se reglamentaron aspectos relativos a la autorización de los titulares, las políticas de tratamiento de la información, las transferencias y las transmisiones internacionales y el principio de responsabilidad demostrada (*accountability*). Este último principio, con referencias de tiempo atrás en legislaciones extranjeras, en esencia se refiere a la obligación de los responsables del tratamiento, no solo de cumplir con sus obligaciones legales, sino de estar en capacidad de demostrar su cumplimiento desde un punto de vista práctico (Alhadeff, Van Alsenoy y Dumortier, 2012). Para cumplir con este principio los responsables deben implementar medidas técnicas, humanas y administrativas apropiadas, a través de políticas internas efectivas acordes con las instrucciones de la Superintendencia de Industria y Comercio (SIC)[11]. La existencia e implementación de estas medidas son consideradas por la SIC al momento de evaluar la imposición de sanciones por infracciones en materia de protección de datos, por lo que el principal reto

11 Artículo 27 del Decreto 1377.

de los responsables es demostrar que su programa es efectivo y apropiado a su organización y se ajusta a la Ley (Remolina Angarita, 2013).

La aplicación del principio de responsabilidad demostrada a partir de las instrucciones de la SIC permite introducir en Colombia unas herramientas de intervención estatal, como las guías para la protección de datos personales, las cuales se refieren, entre otros asuntos, al tratamiento de datos en entornos educativos, en servicios de computación en la nube, para el manejo de incidentes de seguridad y para fines de comercio electrónico, aunque sin lugar a dudas la más relevante ha sido la Guía para la Implementación del Principio de Responsabilidad Demostrada (GIPRD) publicada en 2016, que es frecuentemente invocada por la SIC en sus decisiones, en particular al citar la responsabilidad de los administradores en materia de protección de datos[12], y cuyo objeto es orientar la construcción del Programa integral de gestión de datos personales a cargo de los responsables, en cuanto a los compromisos que deben asumir como organización, y los procedimientos a implementar para acreditar el cumplimiento de sus obligaciones. Y si bien sus lineamientos no tienen rango de ley, ciertamente constituyen cuando menos doctrina que sirve como criterio auxiliar para su interpretación.

A partir de la facultad radicada en cabeza de la SIC, y en consonancia con la posibilidad de intervención del Estado en el sector de las TIC, en particular para proteger los derechos de los usuarios[13], uno de los cuales es el *habeas data*, pareciera que la SIC tiene el camino abierto para impartir instrucciones a los PRST, a los Proveedores de Contenidos y Aplicaciones (PCA), o a cualquier agente de las industrias del sector TIC sobre las medidas apropiadas para el tratamiento de datos personales a través de la emisión de guías específicas en adición a la normatividad general sobre protección de datos. Al respecto, se considera que la facultad conferida en el artículo 27 del Decreto 1377 está restringida a impartir instrucciones sobre lo que se entiende por medidas efectivas y apropiadas, pero en ningún caso podrán restringir o contrariar la Constitución, la ley, y en especial el derecho fundamental del *habeas data*, y para el sector TIC, la Ley 1341 y su regulación. En caso de que alguna instrucción de la SIC, proferida en forma de guía, sea contraria al ordenamiento jurídico aplicable, debería como mínimo poder ser discutida ante la jurisdicción contencioso administrativa a través de la acción

12 Resolución 9804 de 2019 de la SIC en contra de Travel Link S.A.S.

13 Artículo 4.º de la Ley 1341.

de nulidad simple. Debido a la informalidad que ha rodeado la publicación de las guías de la SIC, las cuales están disponibles solamente a través de su sitio web, su carácter vinculante podría ciertamente ser objeto de discusión en las acciones de nulidad que eventualmente se interpongan en contra de decisiones sancionatorias de la SIC que se fundamenten en ellas.

La facultad para ejercer la vigilancia de las actividades de tratamiento de datos personales fue otorgada a la SIC por las Leyes 1581[14] y 1266[15], y es cumplida a través de la Delegatura para la Protección de Datos Personales. En aquellos casos en que la fuente, el usuario o el operador de la información (conforme estos están definidos en la Ley 1266) sea una entidad vigilada por la Superintendencia Financiera de Colombia (SFC), esta ejercerá la vigilancia conforme a las facultades que le son propias según el Estatuto Orgánico del Sistema Financiero.

De las 104 sanciones impuestas en materia de protección de datos en un año calendario, 52 obedecieron a infracciones de la Ley 1266, mientras que las 52 restantes a infracciones de la Ley 1581 (SIC, 2019); un balance inusual que evidencia que cada vez hay más conciencia sobre la protección de datos personales diferentes de aquellos de estricto contenido financiero, crediticio, comercial o de servicios, pero que no se replica totalmente en el segmento de los PRST, donde es posible observar que la mayoría de las decisiones de la SIC en su contra se deben a controversias derivadas del incumplimiento de las obligaciones como fuentes de información a centrales de riesgo crediticio conforme a la Ley 1266.

En materia de otros servicios relativos al sector de las TIC, la SIC también ha mostrado interés en adelantar actuaciones o hacer requerimientos de información, incluso respecto de empresas que no tienen domicilio en Colombia; así, la SIC adelantó actuaciones administrativas y tomó decisiones en contra de grandes empresas de servicios tecnológicas como Facebook[16], Uber[17] o Rappi[18] en materia de protección de datos. Más allá de las consideraciones sobre la competencia legal de la SIC para investigar a algunas de esas compañías (lo que será objeto de mención más adelante), lo cierto es que

---

14 Artículo 19 de la Ley 1581.

15 Artículo 17 de la Ley 1266.

16 Resolución 12192 de 2020 de la SIC en contra de Facebook Inc.

17 Resolución 21478 de 2019 de la SIC en contra de Uber Technologies Inc., Uber B.V y Uber Colombia S.A.S.

18 Resolución 9800 de 2019 de la SIC en contra de Rappi S.A.S.

el creciente tratamiento de datos personales a través de medios electrónicos hace que este sector se encuentre bajo el radar permanente de la autoridad.

Adicional a las competencias de la SIC, en materia del sector TIC es pertinente referirse a la CRC, la cual, como se señaló, es competente para regular el régimen jurídico de protección al usuario de servicios de comunicaciones[19] que incluye el derecho al *habeas data*. En la Resolución 5111 de 2017 de la CRC, por la cual se dispuso el régimen integral de protección de los derechos de los usuarios de servicios de comunicaciones, se incluye la obligación de los PRST de cumplir con las normas vigentes en materia de protección de datos personales en aspectos tales como la autorización de los usuarios para tratar sus datos, las finalidades de dicho tratamiento, los derechos de los usuarios sobre sus datos personales, las condiciones para la revocatoria del consentimiento, entre otros (art. 2.1.5.1). Así mismo, se disponen condiciones particulares sobre la posibilidad y las condiciones para realizar reportes a centrales de riesgo que involucren la información financiera y comercial de los usuarios (art. 2.1.5.2) .

Adicionalmente, la Resolución 5050 de 2016 de la CRC incluye algunas regulaciones que son relevantes para los PRST, como la necesidad de contar con un sistema de gestión de seguridad de la información y protocolos específicos que le permitan, no solo proteger las comunicaciones, sino la información procesada.

La Resolución 5980 de 2020, por la cual se dispuso la eventual aplicación alternativa del *sandbox* regulatorio, no prevé ninguna cuestión específica en materia de protección de datos, salvo que se deben seguir los principios de la Ley 1341 relacionados con la protección por el *habeas data*. En ese orden de ideas, cualquier proyecto debe cumplir los lineamientos de las normas generales en materia de protección de datos, por lo que le corresponderá a la CRC validar que se garantice dicha situación, y en lo posible, sin obstaculizar el propósito ulterior de promover la innovación por la vía de la regulación.

Por su parte, en materia de PCA, a pesar de no haber expedido ninguna regulación particular en cuanto a la protección de los datos personales, en varios conceptos ha señalado: i) que cuando un PCA produzca, genere y/o consolide contenido de un mensaje en el marco de una relación de acceso donde un integrador tecnológico provea infraestructura de soporte con un

---

19 Artículo 53 de la Ley 1341.

PRST, las partes podrán negociar libremente bajo qué rol cada una de ellas administrará las respectivas bases de datos personales, en cumplimiento de los mandatos de la Ley 1581 (CRC, 2019a), y ii) que siempre que los servicios prestados por una aplicación web impliquen el tratamiento de datos personales se deben seguir los lineamientos de la Ley 1581 (CRC, 2019b).

2. PARTICULARIDADES EN MATERIA DE PROTECCIÓN DE DATOS DE DIFERENTES AGENTES DEL SECTOR TIC

Para efectos de analizar la dimensión de las relaciones y problemáticas que se podrían presentar en materia de protección de datos personales que involucren a las TIC, vale la pena traer a colación la siguiente clasificación de relaciones de privacidad formuladas por Walden (2018), usuario-Estado, proveedor de servicio-usuario, suscriptor-usuario[20] y usuario-usuario, las cuales se extrapolarán al caso colombiano en cuanto resulten aplicables.

El acelerado desarrollo tecnológico, la liberalización del mercado de las telecomunicaciones y la aplicación del principio de equivalencia funcional de la Ley 527 de 1999 como fundamento para manifestar el consentimiento por medios electrónicos, han contribuido a que las relaciones entre contrapartes del sector TIC, en lo concerniente a protección de datos personales, se tornen más complejas debido a su crecimiento exponencial y a su uso para desarrollar productos y servicios innovadores, incluso por actores originalmente alejados del entorno digital. Sin embargo, en materia de privacidad no se considerarán las relaciones que los actores del sector TIC puedan tener con contrapartes o grupos de interés por fuera del mundo digital, las cuales se regirán por las normas generales de protección de datos en lo que les aplique.

---

20 Walden se refiere, por este tipo de relaciones, por ejemplo, a aquellas existentes entre un hotel y un huésped quien accede a Internet a través del servicio contratado por aquel con un PRST, o entre un padre y un hijo cuando el primero es el suscriptor. En consideración a que i) la regulación de la CRC en materia de protección de datos no distingue entre usuario y suscriptor, y ii) el suscriptor no asume la condición de proveedor de servicios TIC frente al usuario, este tipo de relación no pareciera hacerse extensible a ninguno de los casos objeto de análisis más adelante. No obstante lo anterior, según corresponda, y en particular cuando existe entre suscriptor y usuario una relación contractual, es recomendable que se prevean las medidas pertinentes para proteger los datos personales de los usuarios sobre los cuales el suscriptor realice algún tipo de tratamiento.

2.1. LOS PRST Y SU RELACIÓN CON USUARIOS

Para efectos del presente acápite se considera la definición de servicios de telecomunicaciones existente en nuestra norma, según la cual, son aquellos ofrecidos con el fin de satisfacer necesidades específicas de telecomunicaciones a terceros por un PRST, entendido este como la persona jurídica responsable de la operación de la red o de la provisión del servicio de telecomunicaciones respectivo. Lo anterior no incluye a los prestadores de servicios *Over The Top Media Services* (OTT), los cuales, bajo la ley colombiana, no ostentan la calidad de PRST, y cuyas particularidades serán objeto de análisis más adelante.

Entonces, a partir de esa noción de servicios de telecomunicaciones es posible identificar que, para los efectos de la regulación del sector, el tipo de relación de privacidad más relevante es aquel que se realiza entre el proveedor del servicio y el usuario, esto es, quien efectivamente utiliza los servicios, independientemente de que sobre la misma persona concurra también la condición de suscriptor. Al respecto, los derechos y obligaciones del suscriptor del contrato en su calidad de usuario se deben extender también a otros usuarios que se beneficien del servicio de telecomunicaciones, salvo en aquellos casos en que excepcionalmente la regulación señalase que sólo el suscriptor es titular de determinados derechos.

Lo anterior, no obstante que los PRST también puedan eventualmente tratar información personal de los usuarios y suscriptores para finalidades diferentes de la prestación del servicio de telecomunicaciones como, por ejemplo, aquella relativa a sus datos de identificación o medios de pago; dicha relación no sería diferente de la que se tiene con ocasión de la prestación de un servicio, incluso fuera de línea[21]. En lo que respecta a dicho tratamiento aplicarían las normas generales en materia de protección de datos. En ambos tipos de tratamiento la protección a los usuarios y suscriptores, según cada uno de los regímenes aplicables, será extensiva solamente a las personas naturales.

---

21 Si el tratamiento de datos que surte el PRST para efectos de aspectos ajenos a la prestación misma del servicio de telecomunicaciones se provee por medios digitales, podría eventualmente identificarse una relación del tipo usuario-usuario entre el PRST y el usuario; por ejemplo, el ofrecimiento de un canal digital para la atención de PQRS en el cual se traten los datos de los usuarios.

Específicamente en materia de protección de datos que involucran servicios de telecomunicaciones, la regulación colombiana no ha desarrollado en profundidad la calidad que asumirían los PRST respecto de cierta información relativa al servicio y, en particular, respecto de los usuarios y los suscriptores. La regulación de la CRC no distingue entre obligaciones de los PRST como responsables o como encargados, por lo que la misma podría ser aplicable independientemente de la calidad que ostenten.

Bajo el contexto tradicional de los servicios de comunicaciones un PRST probablemente sería caracterizado como responsable de la información del suscriptor y de los datos de tráfico, y como encargado lo sería del contenido que transmite por cuenta de sus usuarios (Walden, 2018). Las obligaciones del PRST en materia de protección de datos dependerán del rol que asuma, por lo que es recomendable que ante la falta de una regulación expresa que determine las condiciones de tratamiento en el contexto de servicios de telecomunicaciones, en los contratos que suscriban con sus suscriptores se regulen las condiciones específicas que deberían aplicar, según los distintos tipos de relaciones entre un PRST y un titular de datos personales.

Adicionalmente, es relevante analizar las obligaciones que se pueden derivar para un PRST respecto del procesamiento de datos que se ajusten a las definiciones de dato de tráfico[22] o de dato de localización[23]. Al respecto, la regulación de la CRC, en particular en lo relativo a las medidas de seguridad aplicables, prohíbe que los PRST entreguen a su arbitrio datos de cualquiera de las dos categorías señaladas, salvo que tengan una autorización expresa y escrita del usuario. Este tipo de información, que por sí sola podría tornarse irrelevante, en conjunto adquiere una dimensión que merece ser objeto de protección, pues podría eventualmente revelar aspectos de la vida privada y de la intimidad de una persona (Fernández Rodríguez, 2016). Respecto de las anteriores categorías de información, la Directiva 2002/58/CE del Parlamento Europeo y el Consejo de la Unión Europea (Directiva sobre la Privacidad y las Comunicaciones Electrónicas) dispone obligaciones particulares a los PRST con miras a proteger la privacidad de los individuos,

---

22 De acuerdo con la Resolución 5050, será toda: "Pieza de información tratada a efectos de la conducción de una comunicación o de la facturación de la misma. Dentro de esta clase de datos se encuentran, entre otros, los datos necesarios para identificar el origen de una comunicación, el destino de la misma, la fecha, la hora, la duración de la comunicación y el tipo de comunicación".

23 De acuerdo con la Resolución 5050, será: "Cualquier pieza de información que permita identificar la ubicación geográfica del equipo terminal de un usuario de servicios de comunicaciones".

de manera similar a aquellas que se imponen para categorías especiales de datos personales (Walden, 2018), por ejemplo, que los datos de tráfico deban eliminarse o anonimizarse cuando ya no sean necesarios para la transmisión de una comunicación electrónica, y que solamente se podrán conservar cuando su finalidad involucre la facturación para los suscriptores o los pagos de interconexión, o la imposición de reglas para su tratamiento en lo relativo a la promoción comercial de servicios de comunicaciones electrónicas. Sin embargo, en Colombia no existe regulación equiparable sobre la materia.

Por otra parte, en cuanto a la seguridad en el tratamiento de la información, en un sentido similar al previsto en la Resolución 5050, la Directiva 2002/58/CE incluyó obligaciones para los PRST y procedimientos a seguir en caso de incidentes de seguridad. Dada la duplicidad normativa para los PRST con ocasión de la expedición del RGPD, en el que también se impusieron medidas que tendrían efectos similares, actualmente existe una propuesta de reglamento europeo que derogaría la Directiva 2002/58/CE, y eliminaría las obligaciones sectoriales de seguridad, de manera que todos los responsables, sin distinción, se adecuen a las directrices del RGPD[24].

Mientras que en otras jurisdicciones el foco en materia de protección de datos por los PRST está dirigido a observar las cuestiones propias de su función como herramienta de transmisión de información, en Colombia la discusión ha tomado otro rumbo. Al observar las decisiones publicadas por la SIC en su portal web con ocasión de algunas actuaciones administrativas en contra de PRST en materia de protección de datos, se observa que alrededor del 85 % se relaciona con controversias propias de la Ley 1266 de 2008, y en particular, con reportes de información negativa de usuarios a centrales de riesgo crediticio.

La anterior situación, que demuestra que la prioridad de los usuarios por ahora es el estado de la información relativa a su salud crediticia, no debe hacer perder de vista que, debido a la gran cantidad de información de las personas a las que los PRST tienen acceso, su tratamiento merece especial atención. Así pues, aun cuando los usuarios no demanden la protección de información diferente de aquella de contenido comercial, es responsabilidad

---

24 Numerales 1.2 y 3.5 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas, y por el que se derogaría la Directiva 2002/58/CE (Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas).

de las autoridades competentes velar y garantizar que cualquier tipo de información que pueda tener la potencialidad de identificar a una persona o sus hábitos sea objeto de protección.

2.2. LA CONTRATACIÓN Y EJECUCIÓN DE SERVICIOS A TRAVÉS DE MECANISMOS DE COMUNICACIÓN ELECTRÓNICA

A continuación se analizan algunos actores del sector TIC, diferentes de los PRST, pero cuyo énfasis ha sido la utilización de los servicios de telecomunicaciones, en particular de la Internet, para efectos de prestar servicios, así como distribuir distintos productos a sus consumidores. Bajo dicho marco, a partir de la definición vigente de telecomunicaciones en el régimen colombiano, al no estar frente a un PRST las relaciones de privacidad que se analizan a continuación parecieran encuadrar en aquellas denominadas usuario-usuario, en el sentido de que ambas partes son usuarias de servicios provistos por un PRST como premisa para concurrir en la relación que les incumbe; es decir, tanto el proveedor del servicio OTT como el usuario del mismo deben contar, cada uno, con acceso a servicios de telecomunicaciones que les permitan, respectivamente, ofrecer o acceder al servicio en cuestión.

2.2.1. LOS SERVICIOS *OVER THE TOP MEDIA SERVICES* (OTT)

En primer lugar corresponde analizar los servicios OTT, categoría que comprende los servicios ofrecidos por jugadores diferentes de los PRST que se nutren del servicio de Internet prestado por estos, y que permiten satisfacer ciertas finalidades de comunicación que originalmente solo era posible atender a través de PRST como, por ejemplo, la comunicación de contenido audiovisual o la transmisión de voz y mensajería instantánea (SMS) (Hidalgo Viedma, 2019). En este tipo de servicios no existe control o gestión alguna de los PRST, y en todo caso se requiere que el usuario final cuente con su propia conexión a Internet. La principal preocupación que generan al mercado es que, a pesar de que presentan funcionalidades similares a servicios prestados por los PRST, no están sujetos a la misma regulación (Given y Carey, 2018).

Para el caso colombiano, y en particular en materia de protección de datos, no se han desarrollado normas particulares relativas a las condiciones

del tratamiento que debe ser cumplido por los prestadores de servicios OTT pues, en razón a que no cuentan con la calidad de PRST, no están obligados a cumplir con aquellas obligaciones derivadas del régimen de protección de usuarios de la Ley 1341. A lo sumo, entonces, como cualquier otro responsable o encargado del tratamiento, un proveedor de servicios OTT deberá cumplir, en lo que le resulte aplicable, las normas generales de protección de datos personales y los lineamientos definidos por las autoridades en cuanto resulten pertinentes.

A pesar de que en otras jurisdicciones los servicios OTT no han sido íntegramente equiparados con los servicios de los PRST, sí se ha reconocido su relevancia como posible sustituto. Así las cosas, por ejemplo, dentro de la propuesta de reglamento que derogaría la Directiva 2002/58/CE (la propuesta de reglamento sobre la privacidad y las comunicaciones electrónicas), y en consonancia con la definición de comunicaciones electrónicas contenida en el Código Europeo de las Comunicaciones Electrónicas[25], se señala que las comunicaciones transmitidas a través de nuevos servicios, como los OTT (p. ej., servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico basados en la web) están desprovistas de protección[26], y al contener una funcionalidad de comunicación deben quedar cubiertas por las normas que se dicten en materia de protección de datos.

De conformidad con estudios recientemente publicados (CRC, 2020) no se anticipa la expedición de alguna norma que tenga por objeto la regulación de los servicios OTT, y mucho menos la expedición de alguna norma particular que tienda a imponer obligaciones a los respectivos prestadores en materia de protección de datos.

En consecuencia, para los efectos del cumplimiento de la ley, los proveedores de servicios OTT serán responsables del tratamiento de los datos personales de sus suscriptores, sin perjuicio de que, en determinadas circunstancias y a partir de las condiciones contractuales del servicio, puedan asumir la calidad de encargados de los datos personales de algún usuario respecto del cual el suscriptor actúe como responsable.

---

25 Directiva (UE) 2018/1972 del Parlamento Europeo y el Consejo de la Unión Europea.

26 Numeral 1.1 de la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas.

2.2.2. LA CONTRATACIÓN A TRAVÉS DE PLATAFORMAS DE COMERCIO ELECTRÓNICO

No obstante que la contratación electrónica no se limita a las transacciones que realizan los consumidores a través de portales o plataformas web, pues ciertamente su utilidad se extiende incluso para la contratación que no tenga la calidad de una relación de consumo (Rincón Cárdenas, 2020), dada su relevancia en lo que respecta a la protección de datos personales por los volúmenes de información que implican, las consideraciones a continuación se referirán de manera exclusiva a las relaciones de consumo que se concretan por esa vía.

En este acápite se hará referencia a aquella nueva metodología para celebrar transacciones comerciales, que ha sido desarrollada gracias a las herramientas legales previstas en la Ley 527 de 1999, y que, entre otras características (Rincón Cárdenas, 2020): i) se realizan a través de un canal que permite la comunicación electrónica soportada en mensajes de datos, entendidos estos, como documentos en formato electrónico que acreditan determinada información (Peña Valenzuela, 2015); ii) las partes no deben coincidir necesariamente en el mismo lugar; iii) la prueba idónea de la manifestación de la voluntad no será, en principio, un registro impreso de la transacción, y iv) permite globalizar la prestación de bienes y servicios.

En este tipo de relaciones el proveedor del bien o el servicio sin duda actuará como responsable del tratamiento del consumidor que sea persona natural. En lo que respecta a transacciones en las cuales la parte adquirente es una persona jurídica, una primera consideración sería, en cuanto resulte posible, abstenerse de solicitar información de personales naturales, y que cuando sea necesario hacerlo para la ejecución de la relación contractual, se dispongan las medidas para que el tratamiento por el proveedor, sea en calidad de responsable o de encargado, se haga dentro de una de las bases legitimadoras existentes en Colombia.

Las relaciones de privacidad en la operación de una estrategia de comercio electrónico, en particular cuando la misma se realiza a través de una plataforma digital propia (o incluso a través de un *marketplace*)[27], pueden implicar la circulación de los datos personales entre muchos de los sujetos

---

27 En particular para el caso de los *marketplaces*, también remitirse a la sección de intermediarios de información en Internet de este capítulo.

involucrados; por ejemplo, en el proceso de comercialización y distribución de servicios y productos, además del comerciante mismo, podrían intervenir terceros tales como operadores de las plataformas, pasarelas de pago, proveedores de servicios de almacenamiento en la nube, o *call centers*, entre otros. Lo anterior impone a los proveedores de productos y servicios a través de canales electrónicos, la obligación de garantizar que desde el momento de la planeación de la estrategia de comercialización se implementen los procedimientos y medidas de seguridad adecuadas conforme su operación específica que garanticen la protección de los derechos de los titulares de datos personales.

Al respecto, en 2019 la SIC emitió la Guía sobre el tratamiento de datos personales para fines de comercio electrónico, en la cual se dictan algunas pautas para la implementación de estrategias relacionadas con tal finalidad, entre ellas: i) identificar el alcance territorial y cumplir con las leyes locales aplicables; ii) exigir a los terceros que soportan su estrategia el respeto de su Política de Tratamiento de Información (PTI); iii) efectuar estudios de impacto de privacidad sobre la cantidad y el tipo de datos personales, y el tipo de tratamiento que se cumplirá; iv) implementar estrategias de privacidad por diseño y por defecto a partir de los resultados de los estudios de impacto; v) implementar medidas para evitar la suplantación de identidad de los consumidores; vi) garantizar la seguridad de la información de los consumidores; vii) recolectar los datos estrictamente necesarios para fines de comercio electrónico, y viii) obtener datos personales lícitamente y para las finalidades respectivas. En cuanto a este tipo de instrumentos de la SIC, aun cuando se pudiera discutir su carácter vinculante, como se indicó atrás, no se debe perder de vista que constituyen interpretaciones e instrucciones de la autoridad competente que sirven de guía para responsables y encargados.

La implementación de una estrategia de comercialización de una empresa a través de medios electrónicos no necesariamente va a ser idéntica o siquiera similar a la de otra. En ese orden de ideas, en cada caso es necesario que la operación de la plataforma esté articulada con la operación de la respectiva empresa, y que en lo relativo al tratamiento de datos personales se establezcan los procedimientos internos de acuerdo con el tipo de tratamiento que tiene lugar al interior del responsable, así como aquel que pueda involucrar la entrega de datos personales a terceros a título de transmisión o de transferencia.

Así mismo, en el evento de que, con ocasión de la recolección de información personal que se surte como parte de la estrategia de comercio electrónico,

ella sea objeto de análisis agregado junto con otra información del mismo titular o de otros, con miras a, por ejemplo, identificar hábitos de consumo, o generar resultados que permitan la toma de decisiones corporativas, una manera de mitigar los riesgos es minimizar el uso de los datos personales para ese tipo de estrategias o, en cuanto sea posible, implementarlas a través del uso de información anonimizada a partir de la cual no sea posible individualizar al titular respectivo.

En general la operación de una plataforma de comercio electrónico supone múltiples riesgos según el tipo de datos personales que involucre y el tratamiento que se les dé, por lo que en cada caso el responsable deberá implementar las medidas respectivas que mitiguen cualquier riesgo en su contra y promuevan la efectiva protección de los derechos de los titulares.

2.2.3. LOS CONTRATOS INTELIGENTES

En materia de contratación a través de comunicaciones electrónicas, y dado el creciente interés en su uso, se debe hacer referencia a los denominados contratos inteligentes a través de registros distribuidos agrupados en una cadena de bloques (*blockchain*). Esta tecnología, cuya operación se soporta a su vez en la Internet y en protocolos de comunicación entre los participantes, corresponde a una red global de ordenadores (nodos) que gestionan de manera descentralizada, es decir, sin el control de una entidad central que valide todos los procesos, una gigantesca base de datos que puede estar abierta al público o limitada a ciertos participantes (Preukschat, 2017). Para su funcionamiento, como medida de seguridad, se utilizan técnicas criptográficas cuyo propósito es proveer un mecanismo de codificación segura, evitar la manipulación, el robo o la inclusión de información errada en la cadena de bloques, así como generar firmas e identidades digitales (Preukschat, 2017).

De forma que, en esencia, un contrato inteligente es la programación de una lógica codificada que, a través del procesamiento de un determinado conjunto de insumos o condiciones puede generar diversos resultados; su "inteligencia" radica en su capacidad de automatización en tanto su sustancia y ejecución dependen de algoritmos (Delgado de Molina Rius, 2020). En resumen, este tipo de operaciones permite la realización de transacciones a partir de la información almacenada en la *blockchain* (Suda, Tejblum y Francisco, 2017).

Como parte de las discusiones en torno a la legalidad de estas figuras, y dada la posibilidad de que de alguna manera los registros de la *blockchain*

permitan individualizar a una persona natural, su eventual aplicación se torna relevante en materia de protección de datos personales. Sus promotores manifiestan que la privacidad es uno de sus pilares, y que sus protocolos de seguridad permiten elegir a cada titular el nivel de protección de su información personal en cada transacción o entorno donde participe, lo anterior, en parte, debido a que la *blockchain* "no necesita saber quienes somos" (Tapscott y Tapscott, 2017). Por supuesto, este tipo de afirmaciones debe ser tomado con mesura, y ante la imposibilidad de anticipar el verdadero impacto de la tecnología *blockchain*, su evolución debe ser permanentemente monitoreada para identificar qué tendencia regulatoria se debería implementar.

En Colombia no existe ningún referente normativo particular en materia de protección de datos para el caso de la *blockchain*, por lo que cualquier análisis deberá partir de las premisas de la Ley 1581 y sus normas reglamentarias. Al respecto se han planteado diferentes puntos de tensión en materia de regulación de la protección de datos y de la operación de la *blockchain*, los cuales se estiman relevantes a efectos de cualquier análisis sobre la misma (Finck, 2019), incluso en el marco de la Ley 1581:

– Una red descentralizada soportada en nodos a nivel global representa un reto para legislaciones en las que la competencia de las autoridades de vigilancia y control tenga un alcance territorial restringido.

– La identificación del responsable o los responsables conjuntos, o de los encargados que puedan concurrir en su operación es determinante, pues al ser bases de datos distribuidas, varios actores pueden participar en el tratamiento de la información.

– En un sistema en el que la modificación unilateral de información es una dificultad, podrían existir inquietudes sobre la manera a través de la cual se garantizará el ejercicio de los derechos por parte de los titulares, y en especial, el derecho de supresión.

Si bien la tecnología *blockchain* ha sido calificada como una herramienta que ofrece mayor seguridad para el tratamiento de datos personales (Zyskind, Nathan y Pentland, 2015), su idoneidad *versus* las distintas leyes de protección de datos será objeto de revisión en los años por venir. Este tipo de tecnología es cada vez más utilizado para la administración y verificación de datos en sectores gubernamentales, aseguradores y de salud (Zīle y Strazdiņa, 2018); incluso en Colombia ha sido considerada por la Agencia Nacional de Tierras (ANT, 2018) para gestionar información relativa a la adjudicación de terrenos baldíos.

Ante la actual incertidumbre sobre su impacto real, y en particular, sobre el alcance de su aplicación en el marco de la regulación de protección de datos, cualquier aproximación regulatoria apresurada podría impedir su adecuado desarrollo. En tal virtud, la aplicación escalonada de acciones mediante el acompañamiento de la autoridad a los procesos de creación de los desarrolladores, así como el incentivo a la aplicación de los principios de protección de datos, de prácticas de privacidad por diseño y por defecto, y de prácticas de minimización en el uso de datos personales, pueden contribuir a su correcta implementación garantizando la protección de los titulares.

2.2.4. LOS INTERMEDIARIOS DE INFORMACIÓN EN INTERNET

Ciertamente el concepto de intermediario de contenidos ha cambiado gracias a la utilización de la Internet. Por intermediario se entiende quien actúa entre el sujeto que presenta una información y la audiencia que la recibe, y que, además, provee una herramienta para que el contenido le llegue a esta última (Rowbottom, 2018); en materia de intermediarios digitales este concepto incluye, entre otros, a los proveedores de acceso a Internet, los motores de búsqueda, los intermediarios de comercio electrónico (*market-places*), los sistemas de pago por Internet (pasarela de pago) y las plataformas participativas que permiten la publicación de contenido por terceros sin, en principio, crear o tener los derechos sobre esa publicación (redes sociales) (OCDE, 2011).

No obstante las responsabilidades que le caben a cada uno de los intermediarios en aquellos eventos en que actúen como responsables o encargados del tratamiento de datos personales en situaciones específicas y ajenas propiamente a la intermediación, por ejemplo, en la relación con sus usuarios u otros grupos de interés, gran parte de la discusión en materia de protección de datos y privacidad se ha centrado en su responsabilidad sobre los contenidos que publican los usuarios.

En Colombia dicha discusión ha sido repetidamente zanjada por las autoridades judiciales. En particular, la Corte Constitucional[28] ha indicado que los intermediarios de Internet no son responsables por el contenido que

---

28 Corte Constitucional. Sentencia SU-420 del 12 de septiembre de 2019, M. P.: José Fernando Reyes Cuartas.

publican sus usuarios, pues extender dicha carga podría limitar los derechos a la libertad de expresión, por lo que la responsabilidad del contenido publicado será de quien directamente afecta el derecho al *habeas data*. No obstante lo anterior, la Corte Constitucional encontró que en aquellas situaciones en que un juez decida que un contenido atenta contra los derechos fundamentales de una persona, su competencia incluye la posibilidad de ordenar la remoción directamente a los intermediarios para así garantizar los derechos del afectado, por ejemplo, porque el infractor no quiere o no puede cumplir con lo ordenado por un juez, y previo cumplimiento de ciertos requisitos por el actor[29].

Ahora bien, lo anterior no quiere decir que la Corte Constitucional haya declarado que los intermediarios son responsables del tratamiento de datos personales con todas las repercusiones que ello implica, como lo decidió en su momento el Tribunal de Justicia de la Unión Europea (TJUE) en el comúnmente denominado *Caso Costeja*[30]. Al respecto, incluso la Corte Constitucional ha señalado que la sentencia del TJUE no es un precedente vinculante toda vez que se trata de un asunto concreto fallado con base en un cuerpo normativo que no rige en Colombia[31].

En consecuencia, cuando a través de contenidos difundidos por terceros a través de las herramientas provistas por los intermediarios de Internet se vulnere el derecho al *habeas data* de una persona, cualquier acción debe dirigirse en contra del autor o creador del contenido, y no contra aquellos, los cuales, bajo la normatividad colombiana, no contarán con la calidad de responsables del tratamiento de datos personales para esos efectos.

---

29 Ídem. "Entre personas naturales, o cuando sea una persona jurídica alegando la afectación respecto de una persona natural, solo procederá cuando quien se considere agraviado haya agotado los siguientes requisitos: i) Solicitud de retiro o enmienda ante el particular que hizo la publicación. Esto por cuanto la regla general en las relaciones sociales, y especialmente en las redes sociales, es la simetría por lo que la autocomposición se constituye en el método primigenio para resolver el conflicto y la acción de tutela es el mecanismo residual; ii) Reclamación ante la plataforma donde se encuentra alojada la publicación, siempre y cuando en las reglas de la comunidad se habilite para ese tipo de ítem una posibilidad de reclamo; iii) Constatación de la relevancia constitucional del asunto, aun cuando existen la acción penal y civil para ventilar este tipo de casos, no se predica su idoneidad y eficacia cuando así lo demuestre el análisis de contexto en que se desarrolla la afectación".

30 Tribunal de Justicia de la Unión Europea (Gran Sala). Sentencia del 13 de mayo de 2014, Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

31 Corte Constitucional. Sentencia T-277 del 12 de mayo de 2015, M. P.: María Victoria Calle Correa.

La anterior lógica, aplicable en materia de opiniones, es también relevante, por ejemplo, a efectos de determinar la situación de tratamiento de datos de otro tipo de intermediario, como sería una plataforma de *marketplace* en lo que respecta a la información de sus usuarios (vendedor y comprador). En este caso, además del operador de la plataforma, el vendedor del producto también tiene acceso a los datos personales del comprador a título de responsable; adicionalmente, según el tipo de operación del *marketplace*, el operador y el vendedor podrían, directamente o a través de terceros, asumir ciertas obligaciones en las cuales se podrían concretar múltiples operaciones de transmisión o transferencia según sea el caso.

No existe duda respecto de la posición de los intermediarios como responsables del tratamiento de la información de sus usuarios, de forma que la SIC ha tomado decisiones en su contra en situaciones en las que consideró que existieron riesgos para los usuarios, cubriendo incluso a sociedades no domiciliadas en Colombia que operan una plataforma web, en particular, por la información que se recolecta a través de *cookies*[32].

Ciertamente la celebración y ejecución de contratos a través de mecanismos de comunicación electrónica representa retos para los Estados, dado que la extraterritorialidad de las relaciones en muchos casos excede el campo de acción de las autoridades de control. Así mismo, la complejidad de las relaciones contractuales y los flujos de información en las diferentes situaciones descritas, crearán muchas zonas grises en materia de asignación de responsabilidades a los sujetos involucrados y del ejercicio de los derechos por los titulares.

No es exagerado afirmar que el futuro de la contratación civil y comercial estará mayormente soportado en comunicaciones electrónicas, y que los datos personales son un insumo fundamental para ello. Así las cosas, lo deseable es que los regímenes legales permitan el desarrollo de estas nuevas dinámicas contractuales, que se promueva que los responsables, desde su origen, implementen medidas tendientes a proteger los datos que tratan, y se disponga una regulación acorde con la realidad que otorgue certeza a todos los sujetos involucrados. A modo de ejemplo, el reciente Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo de la Unión Europea sobre transparencia para los usuarios profesionales de servicios de intermediación

---

32 Cfr. nota 17.

en línea, resalta la importancia de que, al menos en lo relativo a usuarios profesionales, se establezcan reglas claras en materia de acceso técnico y contractual a los datos personales que se traten.

Las relaciones de privacidad a las que se refiere esta sección son quizá las más escrutadas y que primero se vienen a la mente de los usuarios y las autoridades, pues el uso de las TIC es cada vez más intrusivo en diferentes aspectos de la vida de las personas. Así mismo, el uso de información por los responsables y encargados alrededor del globo, incluidos los datos sensibles, representa un verdadero reto para las autoridades y para los titulares, que se ven enfrentados a situaciones en las que, en muchos casos, no existe otra opción que entregar la información para poder acceder a un servicio, y en las que los textos de autorización son tan pesados y difíciles de comprender que los consentimientos se suelen otorgar sin que medie una lectura previa concienzuda, e incluso con tiempos de lectura de alrededor de un minuto para documentos que deberían tomar más de veinte a un ritmo promedio (Obar y Oeldorf-Hirsch, 2020).

En ejercicio de su rol como autoridad de control de la Ley 1581, para la SIC los agentes que intervienen en este segmento son altamente relevantes, como se observa en algunas de sus decisiones, o en los requerimientos en contra, por ejemplo, i) del administrador de una página alojada en una red social sobre el cual declaró que es responsable del tratamiento de datos personales con las obligaciones legales que ello implica[33]; ii) de plataformas intermediarias de envíos a domicilios con ocasión de los mecanismos para la toma y la prueba de la autorización de tratamiento por el titular[34]; iii) de plataformas intermediarias de Internet cuyos propietarios y operadores no están radicados en Colombia[35]; iv) de un *marketplace* en relación con la obligación de garantizar los derechos de los titulares, y señalar que se presenta una infracción, por ejemplo, al continuar enviando publicidad no obstante que el titular haya solicitado la supresión de sus datos para tales finalidades[36], o v) de una plataforma de comunicaciones soportadas en Internet (SIC, 2020).

---

33 Resolución 54265 de 2019 de la SIC en contra de Wikimujeres S.A.S.

34 Cfr. Resolución 78899 de 2017 de la SIC en contra de Inversiones CMR S.A.S., y nota 19.

35 Cfr. notas 26 y 27.

36 Resolución 28373 de 2018 de la SIC en contra de Linio Colombia S.A.S.

2.3. EL ESTADO COMO AGENTE DEL SECTOR EN COLOMBIA

Sin duda en Colombia el Estado continúa siendo un agente muy importante del sector TIC. No obstante haber limitado en ciertas instancias su intervención como PRST con ocasión del proceso de liberalización, su relevancia es sumamente importante, por lo que, sin distinción de la relación que asuma respecto de los datos de los titulares, sus actuaciones siempre deben estar regidas por la protección de los derechos fundamentales de los ciudadanos, y en cumplimiento de la ley. Sin lugar a dudas, "la gestión estatal no es incompatible con la protección de los datos personales" (Remolina Angarita, 2013), por lo que las entidades públicas y sus funcionarios son ciertamente sujetos de las obligaciones de la Ley 1581 en lo que les resulte aplicable.

A partir de la clasificación del tipo de relaciones de privacidad al que se ha hecho referencia (Walden, 2018), es posible identificar que en Colombia concurrirían varias relaciones de privacidad. En primer lugar, aunque cada vez menos común, es posible observar la relación del proveedor de servicio-usuario. Así mismo, y en consideración al incremento del uso del ofrecimiento de servicios digitales por el Estado a los ciudadanos, también podría concurrir una relación del tipo usuario-usuario. En ambos casos aplicarían las consideraciones presentadas atrás para esos tipos de relaciones.

Sin embargo, en materia de protección de datos existe también el tipo de relación denominada usuario-Estado, la cual parte de las garantías fundamentales de todo ciudadano, y se refiere a la protección de las comunicaciones respecto de interferencias ilegales realizadas por las autoridades. Lo anterior, que guarda relación con otros derechos fundamentales además del *habeas data*, es relevante dado que, a través de medios tecnológicos, ciertas autoridades están en capacidad de obtener, u ordenar la obtención de información personal relativa a los ciudadanos en el marco de sus funciones públicas.

No es el objeto del presente capítulo analizar en detalle las competencias de las autoridades en materia de interceptación de comunicaciones de los ciudadanos; sin embargo, no sobra mencionar que cualquiera que sea el caso, la obtención de información personal a través de los mecanismos con que cuentan, siempre se debe hacer en estricto cumplimiento de la ley y protegiendo los derechos fundamentales de las personas.

El cumplimiento de la Ley 1581 se ha enfocado en el sector privado, mientras que pareciera que el Estado ha actuado de una manera menos diligente

(González, 2019). Con ocasión de la implementación de la cédula de ciudadanía digital y la prestación de servicios ciudadanos digitales, las entidades públicas interoperarán como responsables y encargadas de datos personales, y en particular, deberán cumplir con las siguientes obligaciones[37]:

– Evaluar el impacto del tratamiento de los datos personales antes de iniciar la prestación del servicio.

– Crear e implementar un programa integral de gestión de datos personales, de conformidad con la guía para la implementación de responsabilidad demostrada de la SIC.

– Designar una persona o área para que asuma la función de protección de datos personales.

– Atender las prácticas internacionales en materia de privacidad por diseño y por defecto.

– Contar con una estrategia de seguridad y privacidad que periódicamente evalúe el riesgo de seguridad digital, como parte de su sistema de administración del riesgo operativo.

– Impedir que los datos de los usuarios sean comercializados, o explotados comercialmente, salvo autorización expresa del titular, conforme se prevé en la Ley 1581 de 2012.

Se observa que el reto para el Estado no es menos grande que para el sector privado, y que, con ocasión de la digitalización de sus relaciones con los ciudadanos, las entidades se verá obligada a cumplir ciertos estándares que pueden no estar en capacidad de asumir. Ciertamente, la participación del Estado en el sector de las TIC lo obliga, más allá del ejercicio de control y vigilancia del cumplimiento de la ley, a actuar con la mayor de las diligencias en cada una de las relaciones con los distintos titulares de datos personales, y para el caso de Colombia, sin dejar de observar otros instrumentos, como la Ley 1712 de 2014 en materia de transparencia y acceso a información pública, que podrían poner a los funcionarios en predicamentos en lo que respecta a sopesar diferentes derechos de los ciudadanos.

---

37 Capítulo 5.º del Decreto 620 de 2020: "Tratamiento de datos personales, seguridad y privacidad de la información".

3. TENDENCIAS REGULATORIAS EN MATERIA DE PROTECCIÓN DE DATOS RELEVANTES PARA EL SECTOR TIC

En consideración al estado actual del uso de las TIC, no sorprende que en años recientes se hayan presentado iniciativas legislativas en la materia; sin embargo, las más recientes que han tenido recepción del Congreso son aquellas encaminadas a modificar la Ley 1266[38], en particular, en lo referente a otorgar beneficios a las personas cuyos datos crediticios o financieros son objeto de tratamiento por fuentes y operadores de información.

Con relación a la Ley 1581 se han presentado algunos proyectos infructuosos de reformas. Mediante el Proyecto de Ley número 2016 de 2015 del Senado de la República[39] se pretendía extender el ámbito de la Ley 1581 a responsables y encargados del tratamiento que no residieran ni estuvieran domiciliados en el territorio de Colombia. Por su parte, mediante el Proyecto de Ley número 89 de 2017 del Senado de la República[40], además de la modificación al alcance territorial de aplicación de la Ley 1581, se incorporaban a la misma los principios de protección de datos desde el diseño y por defecto, de responsabilidad demostrada y de proporcionalidad, se regulaba la figura del delegado de protección de datos y en general se incorporaban disposiciones sobre el cumplimiento de obligaciones a cargo de los responsables del tratamiento.

El Gobierno Nacional expidió la Política Nacional para la Transformación Digital e Inteligencia Artificial (DNP, 2019) y la Política Nacional de Confianza y Seguridad Digital (DNP, 2020), y aunque en ambas se resalta la privacidad como uno de los principios que se debe observar, en ninguna de ellas se presentan consideraciones en torno a figuras regulatorias novedosas en materia de protección de datos personales, como sí se hace, al menos tímidamente, en la Política Nacional de Explotación de Datos (*big data*).

No obstante la similitud a nivel global entre ciertos conceptos o lineamientos en materia de protección de datos, en particular a partir de la

---

38 Proyecto de Ley Estatutaria n.º 62 de 2019 del Senado de la República y 314 de 2019 de la Cámara de Representantes según el informe de conciliación contenido en las *Gacetas del Congreso* n.os 280 y 282 de 2020 respectivamente.

39 *Gaceta del Congreso* nº. 820 de 2015 del Senado de la República.

40 *Gaceta del Congreso* nº. 876 de 2017 del Senado de la República.

definición de unos principios muy similares como los de legalidad, finalidad, confidencialidad y transparencia, es posible encontrar algunos en los cuales la normatividad colombiana no guarda identidad con regulaciones extranjeras; si bien lo anterior no necesariamente se traduce en una desprotección de los derechos de los titulares, su estudio es pertinente para efectos de eventualmente analizar su pertinencia en el sistema colombiano.

3.1. Las bases legitimadoras del tratamiento de datos personales y la autorización como regla general

En consonancia con la Ley 1581 de 2012 y las consideraciones de la Corte Constitucional al respecto, el tratamiento de datos personales solamente podrá tener lugar, con la autorización libre, previa, expresa e informada del titular[41]; para la obtención de la autorización se deben cumplir ciertas condiciones de información[42], y conservar su evidencia por cualquier medio que permita su consulta posterior[43]. Solamente en las siguientes situaciones excepcionales la normatividad colombiana permite el tratamiento de datos sin autorización del titular: i) cuando la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; ii) cuando los datos son de naturaleza pública; iii) en casos de urgencia médica o sanitaria; iv) cuando el tratamiento es autorizado por la ley para fines históricos, estadísticos o científicos, y v) cuando la información está relacionada con el registro civil de los titulares.

Mención especial merece en este punto la Ley 1266, la cual, debido a la naturaleza de la información que implica, parte también de la premisa general de la autorización del titular, con algunas excepciones, para que las fuentes de la información puedan utilizarla, circularla y, en general, realizar las actividades de verificación de comportamiento crediticio de los titulares. Como se señaló, las controversias derivadas de la Ley 1266 son el principal foco de actuaciones administrativas de la SIC en contra de los responsables en Colombia, y entre ellas, las relativas a las autorizaciones representan una alta proporción.

---

41 Cfr. nota 1.
42 Artículo 12 de la Ley 1581.
43 Artículo 9.º de la Ley 1581.

Mientras que en Colombia la autorización es la regla general, y las demás bases para el tratamiento son excepcionales, en algunos regímenes extranjeros la primera convive con otras bases que son igualmente legítimas, y no como excepciones. Así las cosas, en su artículo 6.º el RGPD prevé, además del consentimiento del titular, las siguientes condiciones lícitas: i) con ocasión de una necesidad contractual o precontractual del titular; ii) para el cumplimiento de una obligación legal del responsable; iii) para proteger los intereses vitales del titular o de otra persona natural; iv) para cumplir una labor realizada en interés público o en ejercicio de poderes públicos a cargo del responsable, y v) en ejercicio de los intereses legítimos del responsable o de un tercero, siempre que sobre dichos intereses no prevalezcan derechos y libertades del titular.

Por su parte, el CCPA no enlista unas bases legítimas para el tratamiento de datos personales, como lo hacen otras normas, aunque incluye ciertos derechos para los titulares. Esta norma, dirigida a proteger a los consumidores del Estado de California en los Estados Unidos de América, dispone un derecho de exclusión voluntaria (*right to opt-out*) para que el titular instruya al responsable a no vender su información personal. Solamente con respecto a titulares hasta de 16 años de edad se dispone la necesidad de un consentimiento afirmativo y voluntario (*right to opt-in*).

Los tres regímenes revisados incluyen aproximaciones diferentes a las causas que legitimarían el tratamiento de datos personales. El consentimiento expreso como tendencia regulatoria ha dado paso a modelos en los que su exigencia es excepcional o alternativa a otros fundamentos. Como se sugiere en la Política Nacional de Explotación de Datos (*big data*) contenida en el Conpes 3920, debido al creciente procesamiento de volúmenes de información los esfuerzos regulatorios de muchos Estados parecieran enfocarse en establecer reglas sobre los usos permitidos y prohibidos, independientemente de que el titular consienta su tratamiento[44]. Como señala la SIC en las consideraciones de la guía para la implementación del principio de responsabilidad demostrada, las tendencias en materia de protección de datos se dirigen "hacia un modelo que privilegia la gestión del riesgo y la asignación de responsabilidades" en los responsables del tratamiento[45].

---

44 Numeral 2.1. del Conpes 3920.

45 Consideraciones Preliminares de la GIPRD de la SIC.

Cualquier esfuerzo normativo tendiente a modificar la necesidad de obtener la autorización como regla general para el tratamiento de datos personales, no podría ir desligado de la imposición de obligaciones adicionales a los responsables y el otorgamiento de herramientas a los titulares encaminadas a promover la protección de sus derechos. Dicho de otra manera, la autorización debería mantenerse, pero no como regla general para todo tipo de información, sino solamente para aquellos eventos en que la calidad de los datos personales o las finalidades que habrán de aplicárseles así lo ameriten, por ejemplo, cuando se refieren a datos de menores de edad, a datos sensibles, o cuando su comunicación a terceros pueda generar beneficios económicos al responsable. La autorización tiene un verdadero efecto simbólico y reivindicador de la dignidad de las personas y de su libertad para decidir la información que estará disponible (Remolina Angarita, 2013), por lo que su supresión absoluta no debería ser una opción.

No obstante lo anterior, la falta de consentimiento previo y expreso del titular no puede ser entendida como una desprotección de sus derechos, del mismo modo que tampoco puede asumirse que el hecho de contar con autorización supone que la misma fue bien otorgada, o que ello implica que un responsable actuará adecuadamente. En especial, de las bases legitimadoras del RGPD se destaca aquella referida a la necesidad para la "ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales". Es normal que para la ejecución de un contrato voluntariamente celebrado sea necesario que una parte reciba información de la otra para el cumplimiento de sus obligaciones, por lo que cualquier riesgo de falta de autorización expresa estaría de alguna manera cubierta por la voluntad de celebrar y ejecutar el contrato. Al respecto se ha entendido que esta causal aplica entonces siempre que el titular de los datos personales sea parte del contrato, y que el contrato no puede ejecutarse sin tratar esa información (Dehon y Carey, 2018).

Dado el estado actual del régimen de protección de datos en Colombia en materia de autorización, se considera pertinente que en las posibles discusiones futuras respecto de las normas aplicables se revise la pertinencia de implementar bases legitimadores alternativas al consentimiento como, por ejemplo, la posibilidad de tratar los datos para el cumplimiento de un contrato, siempre que dicha situación no implique el desconocimiento de los derechos de los titulares, y se dispongan obligaciones de rango legal en materia de responsabilidad demostrada. En consideración a la existencia

en Colombia de las Leyes 1581 y 1266, cualquier reforma encaminada a habilitar la aplicación de bases legitimadores diferentes al consentimiento podría suponer una revisión de ambos cuerpos normativos.

Ante las pruebas que evidencian los bajos índices de lectura de las condiciones del tratamiento por los titulares (Obar y Oeldorf-Hirsch, 2020), la consideración de bases legitimadoras adicionales con restricciones a los responsables en cuanto a la finalidad de uso de los datos personales no debería considerarse necesariamente como una medida de desprotección de los titulares.

3.2. LOS DERECHOS OTORGADOS A LOS TITULARES

En materia de derechos otorgados a los titulares, no obstante que la Ley 1581 prevé ciertos mecanismos de protección, en particular en el RGPD se encuentran los siguientes que merecen mención especial:

3.2.1. PORTABILIDAD DE DATOS

Conforme con este derecho, cuando el tratamiento se efectúe por medios automatizados, los titulares podrán recibir los datos personales que les incumben y que hayan facilitado a un responsable, a través de un formato estructurado que pueda ser leído en un mecanismo de uso común, de manera que el titular pueda transmitirlo a otro responsable sin que el responsable original pueda impedirlo[46]. El derecho a la portabilidad de datos fue mencionado en el documento Conpes 3920 como uno de los mecanismos que podría contribuir a la armonización del marco jurídico en aras del avance tecnológico[47].

Este derecho se puede ejercer cuando el titular ha facilitado los datos personales con ocasión de su consentimiento, o cuando el tratamiento ha sido necesario para la ejecución de un contrato. Por el contrario, no aplicará cuando el tratamiento tenga una base jurídica distinta del consentimiento o el contrato, por ejemplo, frente a un responsable que trate datos personales en ejercicio de funciones públicas.

---

46 Artículo 20 del RGPD.

47 Línea de acción 5 del Conpes 3920.

El alcance de este derecho, y en especial la posibilidad de su ejercicio, ha generado múltiples inquietudes en cuanto a los datos que pueden no ser considerados como facilitados directamente por el titular (Lloyd-Jones y Carey, 2018). Al respecto las directrices de la Unión Europea sobre el derecho a la portabilidad de los datos señaló que la expresión facilitados solamente incluía i) los proporcionados de forma activa y consciente por el titular, y ii) los facilitados por el titular con ocasión del uso de un servicio o de un dispositivo (Grupo de Trabajo del artículo 29, 2016); para algunos existe controversia acerca del alcance del derecho, en particular la inclusión de los datos referidos en el numeral ii) anterior pues, en su parecer, la norma europea no los incluyó expresamente (Meyer, 2017).

A su vez, aquellos datos que hayan sido inferidos por el responsable a través de un proceso de creación como parte del tratamiento, no estarán cubiertos por este derecho; lo anterior, por supuesto, sin perjuicio de los derechos de acceso y de conocimiento de la existencia de decisiones automatizadas con su información. Al respecto el ICO (la autoridad de tratamiento de datos del Reino Unido), ha recomendado a los responsables del tratamiento que si la voluntad del titular al realizar la solicitud de portabilidad es clara en cuanto a la inclusión de datos personales inferidos o derivados, su entrega sería una buena práctica.

Con respecto a la inclusión de este derecho en la normativa de protección de datos se ha argumentado que, antes que encajar como un derecho fundamental, es realmente una herramienta reguladora mediante la cual se pretenden estimular la competencia y la innovación en mercados soportados en el procesamiento de datos (Graef, Husovec y Purtova, 2018).

Si bien en Colombia no existe el derecho de portabilidad, una figura que podría asimilarse de cierta manera sería el derecho a la portabilidad numérica. Al respecto, la regulación de la CRC prevé, entre los derechos de los usuarios, la garantía de privacidad de la información suministrada en su solicitud de portación. Adicionalmente, se dispone la obligación del PRST donante de abstenerse de realizar prácticas de recuperación de los usuarios durante el proceso de portación. De forma que las disposiciones de la CRC parecen dejar algunos interrogantes sin resolver como, por ejemplo, si, como parte del proceso de portación, el PRST donante debe eliminar parcial o totalmente los datos personales del usuario luego de culminado el procedimiento, o si los datos personales del usuario portado pueden seguir siendo utilizados con posterioridad al proceso para finalidades, como la recuperación del usuario.

3.2.2. DERECHO AL OLVIDO

Las condiciones en que el derecho al olvido está regulado en el artículo 17 del RGPD no tienen paralelo en el marco general de protección de datos personales de la Ley 1581; sin embargo, en materia de la información regulada por la Ley 1266, dicho concepto se ha desarrollado con ocasión de los reportes de información negativa o de incumplimiento de obligaciones por los titulares.

No obstante, la Ley 1581 prevé el derecho de suprimir o cancelar la información a través de la posibilidad de revocar su autorización al responsable de tratamiento. Si bien este derecho no es equiparable con la norma del RGPD, ofrece ciertas garantías a los titulares, y conforme fue declarado por la Corte Constitucional[48], podrá ser ejercido: i) cuando no se respeten los principios, derechos y garantías constitucionales y legales en el tratamiento, caso en el cual, la SIC debe haber determinado previamente las conductas del responsable o encargado contrarias al ordenamiento, y ii) libre y voluntariamente por el titular, cuando no exista una obligación legal o contractual que le imponga el deber de permanecer en la base de datos respectiva.

A pesar de no estar expresamente previsto en la Ley 1581, por vía de tutela, y en particular en materia de responsabilidad de los medios de comunicación y los intermediarios de Internet, se ha discutido la eventual aplicación del derecho al olvido[49]. Sin duda es un asunto que tomará gran relevancia, y respecto del cual cualquier análisis no debe dejar de lado los efectos que su aplicación tenga respecto de otros derechos como la libertad de expresión.

3.2.3. DERECHOS EN MATERIA DE TOMA DE DECISIONES AUTOMATIZADAS

El artículo 22 del RGPD establece el derecho de todo titular a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de su información a través de perfiles que tengan efectos jurídicos sobre su persona o le afecten significativamente. Al respecto, la norma europea se refiere a perfiles que permitan analizar o predecir aspectos relativos al rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses

---

48 Cfr. nota 1.
49 Cfr. nota 33.

personales, la fiabilidad o el comportamiento, o la situación o los movimientos del titular.

Antes que derechos en favor del titular, la norma del RGPD prevé obligaciones en cabeza de los responsables, incluyendo aquellos eventos en que se podrán tomar las decisiones automatizadas, la necesidad de adoptar medidas para salvaguardar los derechos del titular y su pertinencia ante categorías particulares de datos personales en condiciones especiales.

3.3. El alcance territorial del régimen colombiano de protección de datos personales

Con respecto a su alcance territorial, y en particular, su eventual aplicación a responsables y encargados no domiciliados o localizados en Colombia, existen grandes controversias. El artículo 2.º de la Ley 1581 de 2012 dispone que "[…] la presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en el territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales". En la norma transcrita se observa que la legislación colombiana no pareciera tener alcance extraterritorial, y solamente sería aplicable en algunos de los siguientes dos supuestos: i) cuando el tratamiento de los datos personales se efectúa en el territorio colombiano, o ii) cuando, en virtud de un tratado o instrumento internacional, la legislación colombiana le sea aplicable a un responsable o encargado del tratamiento no establecido en el territorio nacional.

En consecuencia, la Ley 1581 no aplicaría respecto de responsables o encargados que no estén domiciliados en Colombia, que no tengan una sucursal, filial o subsidiaria en el país, y que no tengan servidores ni proveedores del servicio de almacenamiento de datos o información en el territorio colombiano. Lo anterior, sin perjuicio de que por vía de un tratado o instrumento internacional se haga extensiva a una sociedad no establecida en el territorio nacional.

No obstante, la SIC ha interpretado la Ley 1581 en el sentido de extender su aplicación a sociedades que tratan datos personales, indistintamente de si lo hacen desde territorio colombiano o desde el extranjero. Así pues, la SIC ha proferido órdenes administrativas en contra de sociedades extranjeras que supuestamente han ocurrido en incidentes de seguridad que involucran

datos personales de los usuarios a nivel global[50], y que tienen presencia en Colombia a través de una sociedad, que si bien no es la competente de operar la plataforma, a juicio de la SIC contribuye al tratamiento de datos de manera tal que justifica la aplicación de la ley colombiana a las sociedades extranjeras.

Otras legislaciones, como el RGPD y el CCPA, explícitamente disponen el alcance extraterritorial de su aplicación en ciertas condiciones. Así, el artículo 3.º del RGPD prevé que dicha norma aplicará "independientemente de que el tratamiento tenga lugar en la Unión o no"; mientras que la CCPA, que aplica a consumidores residentes en California, no limita su aplicación a negocios o responsables localizados en el Estado de California, salvo que todos los aspectos de la conducta comercial tengan lugar "completamente fuera de California"[51], por lo que se ha concluido que su alcance es extraterritorial. La aplicación de cualquiera de los regímenes extranjeros a un responsable o encargado localizado en Colombia deberá ser objeto de análisis según las circunstancias específicas de tratamiento.

El alcance territorial de la Ley 1581 pareciera estar cubierto por un manto de incertidumbre con ocasión de las recientes decisiones de la SIC, lo cual representa un cambio de posición, pues en un concepto proferido en 2014 explícitamente había señalado que la Ley 1581 no se extendía a redes sociales que "no tienen domicilio en Colombia" (SIC, 2014). Lo anterior estaría ratificado por la existencia de proyectos de ley con propuestas tendientes a extender la aplicación de la Ley 1581 a empresas no localizadas en el país.

Ante la actual regulación del alcance territorial de la Ley 1581, su eventual aplicación a un responsable no ubicado en Colombia pareciera estar rodeada de incertidumbres que serán seguramente resueltas en los estrados judiciales, pero que en cualquier caso podrían ser aclaradas de manera definitiva para otorgar más seguridad jurídica, de contar con alguna disposición similar a la incluida en las normas europeas (Newman Pont y Ángel Arango, 2019).

3.4. UNA NORMA ESPECÍFICA PARA EL SECTOR EN TEMAS DE PROTECCIÓN DE DATOS

Además de las guías expedidas por la SIC y algunas directrices de la CRC sobre los PRST, no existen en Colombia instrumentos regulatorios específicos en

---

50 Cfr. notas 17 y 18.

51 Título 1.81.5 del CCPA, sección 1798.145 (6).

materia de protección de datos para el sector TIC. En general las obligaciones a que están sujetos los responsables y encargados son aquellas previstas en las Leyes 1581 y 1266 y sus normas reglamentarias.

En vigencia de la norma de protección de datos anterior al RGDP –la Directiva 95/46/EC–, en la Unión Europea se adoptó la Directiva 2002/58/CE, denominada Directiva sobre la Privacidad y las Comunicaciones Electrónicas, la cual especifica y complementa la norma general de protección de datos europea, y busca ponerse en línea con el tipo de servicios de comunicaciones electrónicas disponibles al público (al momento de su expedición) a fin de garantizar la protección de los derechos a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales, en particular con ocasión de los servicios disponibles a través de Internet, los cuales, a juicio del legislador europeo, introducen nuevos riesgos para los datos personales de los usuarios y de los suscriptores (denominados abonados).

Dado lo amplio de la definición de comunicaciones electrónicas que contiene esta norma, su aplicación ha sido extendida solamente a operadores de telecomunicaciones fijas y móviles (Walden, 2018), incluso en aquellos eventos en que la organización a cargo de la comunicación no sea responsable (Given y Carey, 2018). No obstante, la propuesta de reglamento sobre la privacidad y las comunicaciones electrónicas, que reemplazaría a la Directiva 2002/58/CE, se extiende incluso a herramientas que permiten la comunicación interpersonal a través de "nuevos servicios basados en Internet que hacen posibles comunicaciones interpersonales tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico basados en la web, en lugar de utilizar los servicios de comunicación tradicionales"[52]. Dicho proyecto pretende no solo alinearse con el GDPR, sino cobijar, además de los sujetos que asimilaríamos a los PRST, a aquellos proveedores de servicios funcionalmente equivalentes que no estaban incluidos en el alcance de la norma anterior, y eliminar cualquier referencia a la intervención regulatoria en materia de la relación de suscriptor-usuario (Walden, 2018).

Se observa, entonces, que las dinámicas propias del sector de las TIC han incidido en la necesidad de desarrollar cuerpos normativos específicos. Por ejemplo, la norma europea analizada incluye, entre otras, disposiciones sobre

---

52 Numeral 1.1 de la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas.

la seguridad y la confidencialidad de las comunicaciones, las obligaciones de los PRST relacionadas con el manejo de los datos de tráfico y las reglas en materia del desvío automático de llamadas y calendarios telefónicos. Vale la pena aclarar que algunos de esos puntos son tratados en la regulación colombiana actual, pero no necesariamente a través del prisma de la protección de datos. Así mismo, no se cuenta con un cuerpo compilado que sea de fácil consulta para los usuarios interesados, y por supuesto, que guíe a los sujetos obligados a poner un énfasis en esta cuestión.

La falta de un cuerpo compilado de normas de protección de datos para el sector TIC no puede considerarse por sí misma una fuente de desprotección de los titulares, puesto que, en todo caso, las normas generales establecen derechos a su favor y obligaciones a cargo de los responsables y encargados, las cuales aplicarán indistintamente del sector. No obstante, dada la realidad ineludible de que el tratamiento por medio de los servicios del sector TIC o, en general, a través de comunicaciones electrónicas, podría tener implicaciones en la manera en que los responsables deberían cumplir las obligaciones y la forma en que los titulares podrían ejercer los derechos, la utilidad de unos lineamientos específicos sería una manera de promover la protección de datos personales en el país.

Las referencias a las situaciones específicas descritas en este numeral 4 no son las únicas diferencias que existen en regímenes legales con normas más actuales que la Ley 1581. Mientras que en Colombia existen las figuras de transmisión y transferencia, las cuales tienen implicaciones diferentes, en otros regímenes no se hace distinción entre las dos figuras y las obligaciones que las partes asumen. Así mismo, en otras jurisdicciones no existen figuras como el Registro Nacional de Base de Datos como herramienta de supervisión, pero sí se han desarrollado condiciones particulares enfocadas en que los responsables asuman la administración de los riesgos en el tratamiento, tales como las normas corporativas vinculantes para empresas relacionadas (situación sobre la cual se publicó un proyecto de Decreto durante el segundo semestre de 2021, pero que no había sido reglamentada en Colombia no obstante estar prevista desde 2012 en la Ley 1581) o la posibilidad de obtener certificaciones en materia de protección de datos que acrediten el cumplimiento de lo dispuesto en las normas.

Con posterioridad a la Ley 1581, la realidad legislativa en materia de protección de datos personales, y en particular de aquellos tratados a través de sistemas que permiten la transmisión de información por medios

electrónicos, ha evolucionado de manera tal que es posible concluir que lo adecuado es adelantar una revisión del estado actual y el enfoque de la Ley 1581, la pertinencia de mantener una norma sectorial como la Ley 1266 o de, incluso, desarrollar obligaciones específicas para otros sectores o tipos de tratamiento, de manera que se identifique si las condiciones actuales favorecen la utilización de información como insumo de nuevos productos y servicios en condiciones que garanticen los derechos de las personas.

CONCLUSIÓN

En razón de la oportunidad de su expedición ha quedado en evidencia que la Ley 1581 no incluye disposiciones en materia de protección de datos personales implementadas con posterioridad en otras jurisdicciones, y que se han diseñado en consideración de la nueva realidad tecnológica y el tipo de relaciones que distintos sujetos podrían tener en materia de privacidad como actores del sector TIC.

Al respecto, a pesar de algunas iniciativas legislativas tendientes a actualizar el régimen general de la Ley 1581, estas no se han logrado concretar, y en cambio el principal punto de atención de los usuarios y de las actuaciones de las autoridades en algunos sectores pareciera continuar siendo la protección de la información de carácter comercial, crediticio y financiero. Sin restarle importancia a la protección de dicha información, las demás categorías de información personal son igualmente relevantes, y como tales requieren una protección acorde con la realidad de los diferentes tipos de tratamiento, y con las tendencias regulatorias en aquello que favorezca a los intereses de los usuarios y permita el desarrollo de productos y servicios innovadores por los responsables y encargados.

En aras de promover el aprovechamiento de datos en beneficio de la innovación tecnológica, el Conpes 3920 sugirió la necesidad de hacer algunas revisiones al régimen de la Ley 1581, en particular en materia de las bases legitimadoras y el derecho de portabilidad de datos. Los fallidos proyectos de ley han apuntado a darles rango legal y aplicación general a principios modernos en materia de privacidad, como la minimización, la responsabilidad demostrada y la privacidad por diseño y por defecto. Por otra parte, hay incertidumbre respecto del alcance territorial de la Ley 1581, lo cual es relevante en lo atinente a la posibilidad de que la SIC pueda efectivamente exigir responsabilidad a una compañía basada fuera de Colombia.

Paralelamente se observa cómo algunos regímenes extranjeros diseñan cuerpos normativos específicos a partir de definiciones revisadas en materia de comunicaciones electrónicas que se ocupan de tipos de relaciones que no solo incluyen a los PRST tradicionales, sino a proveedores de servicios como los OTT. Y, finalmente, el Estado dio inicio a un proceso de digitalización de sus servicios ciudadanos en los que el procesamiento de datos personales y la interoperabilidad entre actores jugará un papel determinante.

Como se observa, más allá del avance de las TIC desde la expedición de la Ley 1581, el contexto fáctico de su aplicación es ampliamente diferente al que se tuvo en cuenta para su discusión y aprobación. Por lo anterior, se considera pertinente y adecuado que las instancias oficiales revisen la actual efectividad del régimen general de protección de datos personales, no solo en cuanto a la protección de los titulares, sino a su eficacia como generadora de innovación.

La Ley 1978 no pareciera haber logrado el cometido real de modernizar íntegramente el sector. Si bien es cierto que se implementaron medidas que podrían contribuir a mejorar las condiciones de conectividad de los colombianos, al menos en lo que respecta a la protección de datos, el sector TIC colombiano está pendiente de modernización. No obstante que por vía de una ley ordinaria no se podría haber modificado una ley estatutaria, la expedición de las Leyes 1978 y 2108 como herramientas de modernización parcial debería permitir que la discusión incluya a continuación otros aspectos que requieren mayor certeza jurídica.

No bastan los esfuerzos de la SIC para intentar concientizar a los titulares, los responsables y los encargados de la importancia de proteger los datos personales mediante decisiones particulares o a través de la expedición de guías con lineamientos sobre prácticas responsables. Para efectos de contar con una mayor certeza sobre las obligaciones y derechos en materia de protección de datos es necesario revisar las actuales condiciones legales, de manera que se identifique la necesidad de incluir nuevas relaciones de privacidad a partir del estado actual de las TIC.

En este capítulo se analizaron algunas de las tendencias regulatorias implementadas, principalmente en Europa, en lo que respecta a la protección de usuarios del sector de las TIC que pueden servir de referentes. La eventual aplicación de modelos regulatorios extranjeros al ordenamiento jurídico colombiano no se puede realizar de manera poco rigurosa o a la ligera; no se debe perder de vista que en ciertas ocasiones la efectividad de alguna medida puede depender de la implementación de alguna otra complementaria, por lo

que cualquier análisis se debe hacer articuladamente, de manera que, además de contribuir con la protección de los derechos de los titulares, promueva la innovación en un sector que cada vez es más relevante en la vida de las personas y las dinámicas sociales.

BIBLIOGRAFÍA

LIBROS

Hidalgo Viedma, G. "Prestadores de servicios, *Over The Top*. Normativa aplicable y situación actual", en J. F. Estévez (ed.). *Derecho Digital*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2019.

ocde. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, París, ocde Publishing, 2011.

Peña Valenzuela, D. *De la firma manuscrita a las firmas electrónica y digital*, 1.ª ed., vol. v, Bogotá, Universidad Externado de Colombia, 2015.

Preukschat, A. *Blockchain: la revolución industrial de Internet*, Bogotá, Paidós Empresa, 2017.

Remolina Angarita, N. *Tratamiento de datos personales: aproximación internacional y comentarios a la Ley 1581 de 2012*, Bogotá, Legis Editores, 2013.

Rincón Cárdenas, E. *Derecho del Comercio Electrónico y de Internet*, Madrid, Tirant lo Blanch, 2020.

Rowbottom, J. *Media Law*, Oxford, Reino Unido, Bloomsbury Academic, 2018.

Tapscott, D. y A. Tapscott. *La revolución blockchain: descubre cómo esta nueva tecnología criptográfica transformará la economía global*, Bogotá, Editorial Planeta, 2017.

Walden, I. "Communications Privacy", en I. Walden (ed.). *Telecommunications Law and Regulation*, 5.ª ed., Oxford, Oxford University Press, 2018.

CAPÍTULOS DE LIBROS

Alhadeff, J.; B. van Alsenoy y J. Dumortier. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions", en D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland y H. Postigo (eds.). *Managing Privacy through Accountability* (pp. 49-82), Londres, Palgrave Macmillan, 2012.

Dehon, E. y P. Carey. "Fair, Lawful, and Transparent Processing", en P. Carey (ed). *Data Protection: A Practical Guide to UK and EU Law*, 5.ª ed., Oxford, Oxford University Press, 2018.

Delgado de Molina Rius, A. y V. García Gil. "Los contratos inteligentes o *smart contracts*", en A. Gurrea Martínez y N. Remolina (eds.). *Fintech, Regtech y Legaltech: fundamentos y desafíos regulatorios*, Valencia, Tirant lo Blanch, 2020.

Given, P. y P. Carey. "Electronic Communications", en P. Carey (ed). *Data Protection: A Practical Guide to UK and EU Law*, 5.ª ed., Oxford, Oxford University Press, 2018.

Lloyd-Jones, H. y P. Carey. "The Rights of Individuals", en P. Carey (ed). *Data Protection: A Practical Guide to UK and EU Law*, 5.ª ed., Oxford, Oxford University Press, 2018.

ARTÍCULOS DE REVISTAS ACADÉMICAS

Fernández Rodríguez, J. J. "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional* (108) 2016, 93-122.

Finck, M. "Blockchain and the general data protection regulation: *Can distributed ledgers be squared with European data protection law*?, Bruselas, Oficina de Publicaciones de la Unión Europea, 2019.

González, X. "De 48.354 entidades, solo 68,7 % registraron sus bases de datos ante la sic", *Asuntos Legales*, 2019.

Graef, I.; M. Husovec y N. Purtova. "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *German Law Journal*, *19* (6), 2018, 1359-1398.

Newman Pont, V. y M. P. Ángel Arango. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*, 48.ª ed., 2019.

Obar, J. A. y A. Oeldorf-Hirsch. "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services", *Information, Communication & Society*, 23(1), 2020, 128-147.

Suda, M.; B. Tejblum y A. Francisco. "Chain Reactions: Legislative and Regulatory Initiatives Related to Blockchain in the United States", *Computer Law Review International*, *18*(4) , 2017, 97-103.

Zyskind, G.; O. Nathan y A. Pentland. "Decentralizing privacy: Using Blockchain to protect personal data", *2015 ieee Security and Privacy Workshops*, San José, CA, EE. UU., 2015.

Zīle, K. y R. Strazdiņa. "Blockchain Use Cases and Their Feasibility", *Applied Computer Systems*, 23, 2018, 12-20.

DOCUMENTOS INSTITUCIONALES

crc. Radicación: 2019522678, 2019a, disponible en [https://www.crcom.gov.co/recursos_user/Normatividad/conceptos_2019/2019522678.pdf].

crc. Radicación: 2019526835, 2019b, disponible en [https://www.crcom.gov.co/recursos_user/Normatividad/conceptos_2019/2019526835.pdf].

crc. "El rol de los servicios ott en el sector de las comunicaciones en Colombia, 2019", Bogotá, 2020.

dnp. Documento Conpes 3920. "Política Nacional de Explotación de Datos (*big data*)", Bogotá, 2018.

dnp. Documento Conpes 3975. "Política Nacional para la Transformación Digital e Inteligencia Artificial", Bogotá, 2019.

dnp. Documento Conpes 3995. "Política Nacional de Confianza y Seguridad Digital", 2020.

Grupo de Trabajo del Artículo 29. "Directrices sobre el derecho a la portabilidad de los datos", Bruselas, Oficina de Publicaciones de la Unión Europea, 2016.

sic. *Radicación: 14-218349- -00003-0000*, Bogotá, 2014, disponible en [https://servicioslinea.sic.gov.co/servilinea/ServiLinea/ConceptosJuridicos/Conceptos/0].

sic. "Informe de rendición de cuentas a la ciudadanía. Balance de Gestión: Agosto De 2018 A Julio De 2019", Bogotá, 2019, disponible en [https://www.sic.gov.co/rendicion-de-cuentas-sic-2019].

sic. "Superindustria investigará plataforma de videoconferencias Zoom para establecer si protege adecuadamente datos de los colombianos", 2020, disponible en [https://www.sic.gov.co/slider/superindustria-investigar%C3%A1-plataforma-de-videoconferencias-zoom-para-establecer-si-protege-adecuadamente-datos-de-los-colombianos].

ESTUDIOS ACADÉMICOS DIGITALES

ANT. "Prototipo Blockchain Tierras", 2018, disponible en [https://www.agenciadetierras.gov.co/transparencia-y-acceso-a-la-informacion-publica/informacion-de-interes/prototipo-blockchain-tierras#documentos].

MEYER, D. "European Commission, experts uneasy over WP29 data portability interpretation", 2017, disponible en [https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/].

Universidad Externado de Colombia

Las Tecnologías de la Información y las Comunicaciones (TIC) han irrumpido en forma vertiginosa en todos los sectores de la nueva sociedad de la información y del conocimiento, de forma que ya no es posible entender los entornos de la sociedad actual sin analizar y comprender cómo ha sido permeada por estas tecnologías que conectan a los ciudadanos a través de las telecomunicaciones.

Diez años después de expedida, la Ley de TIC se reformó mediante la Ley 1978 de 2019. Estos dos acontecimientos justifican el nuevo proyecto investigativo que hoy presentamos a consideración de los lectores con el propósito de que conozcan sus contenidos, sus finalidades, sus aciertos, sus eventuales desaciertos y las mejoras que se pueden incorporar. Esta obra tiene como objetivo inicial analizar el nuevo marco normativo y las reformas introducidas con la Ley 1978 de 2019, muy orientadas al sector de las telecomunicaciones. La investigación se orienta a estudiar el derecho de la competencia en el sector de las TIC, así como los nuevos retos que la sociedad digital y las tecnologías disruptivas le plantean a la sociedad y al derecho administrativo en Colombia.

En consideración a su relación temática, y con el fin de facilitar su organización y lectura, la presente obra se divide en dos tomos: el primero relacionado con *Las TIC y las telecomunicaciones y el derecho a la competencia*, y el segundo referido al *Ecosistema digital en sus distintos desarrollos y las tecnologías disruptivas*.

No cabe duda de la importancia de esta obra, tanto para los lectores especializados como para los interesados en el sector de las TIC y las telecomunicaciones, y de su aporte para el análisis de las instituciones que lo conforman: los proveedores de redes y servicios de telecomunicaciones, los proveedores de plataformas y servicios TIC, los usuarios y todos aquellos que de una u otra forma intervienen en la sociedad del conocimiento virtual.