LA RESPONSABILIDAD CIVIL DEL MANEJO DE DATOS EN LA ERA DIGITAL DESDE LA PERSPECTIVA DE LA NORMATIVA JURÍDICA COLOMBIANA Y DEL MARCO NORMATIVO EUROPEO

Por: ÁNGELA MARÍA LONDOÑO ZAPATA[1]
DANIELA LÓPEZ VALENCIA[2]

RESUMEN

El presente artículo expone la evolución que ha tenido el habeas data en su núcleo esencial por factores externos, como son las nuevas tecnologías y la implementación de nuevas técnicas de mercado, a tal punto de ser considerado actualmente como un derecho fundamental, denominación que, en conjunto con los avances tecnológicos, permite desarrollar un objeto de estudio comparado entre las legislaciones de la Unión Europea y colombiana, identificando así el régimen de responsabilidad establecido por cada una de las legislaciones frente al tratamiento de datos personales, permitiendo establecer similitudes y diferencias entre estas.

Palabras clave

Datos personales, responsabilidad proactiva, responsabilidad subjetiva, tratamiento de datos y big data.

ABSTRACT

This article displays the evolution habeas data has had in it's essencial core by external factors such as new technology and the implementation of new market techniques to such degree that is has actually been considered as a fundamental right. This assignation along with the technological advances allows to develop an object of study compared along legislations from the European Union and Colombia, identifying the regimen of responsibility established by each of the legislations to the treatment of personal data allowing to establish similarities and differences between them both.

[1] Abogada egresada de la Universidad Libre, Seccional Pereira. Estudiante de la Especialización en Derecho de Daños y Responsabilidad Pública y Privada. Contacto: angelalondo75@gmail.com

[2] Abogada egresada de la Universidad Libre, Seccional Pereira. Estudiante de la Especialización en Derecho de Daños y Responsabilidad Pública y Privada. Contacto: danilv17@gmail.com

Keyword

Personal data, proactive responsibility, subjective responsibility, data treatment and big data.

INTRODUCCIÓN

En la dialéctica del mundo contemporáneo la relación del ser humano con la tecnología ha dado grandes cambios, a tal punto de establecer relaciones comerciales y jurídicas sin existir contacto directo entre las partes, lo que ha permitido la creación de nuevos productos y servicios intangibles en los cuales los datos personales se convierten en materia prima que dinamizan el sector económico digital.

Dentro de este campo digital surge el término *big data*, que se refiere al conjunto de datos estructurados o no, cuyo volumen, complejidad y velocidad de crecimiento se debe a la utilización de medios tecnológicos como sensores vinculados en los dispositivos, redes sociales, búsquedas en internet, teléfonos inteligentes y otra variedad de dispositivos o aplicaciones a los que el usuario ingresa cualquier cantidad de datos; la importancia del *big data* radica en la utilización de los datos, de los cuales se desprende un análisis que conlleva a resolver problemas y tomar mejores decisiones a las empresas en dirección al movimiento estratégico de sus negocios (POWERDATA, 2019).

Es por lo anteriormente expuesto que los datos actualmente tiene tanto valor económico y estratégico para las empresas; es así como escándalos de Cambridge Analítica y Facebook en las últimas elecciones han tenido tanta relevancia en el mundo de la seguridad tecnológica y el derecho, haciendo evidente una realidad que estaba a la sombra del *boom* de las redes sociales y las innovaciones tecnológicas. Incluso en Colombia se evidencia la incomodidad de los usuarios al ser contactados por entidades a las cuales nunca han dado la información de su teléfono o han contactado para obtener sus servicios o productos, siendo esta una realidad que nos trae las aplicaciones de los nuevos artefactos y comodidades de la revolución tecnológica, teniendo la ley que desplazarse a este nuevo terreno en aras de proteger los derechos fundamentales.

En cuanto a la protección de los datos personales, la Constitución de 1991, la consagra como derecho fundamental, al afirmar que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…) (art. 15).

Posteriormente, con la Ley Estatutaria 1266 (Congreso de la República de Colombia, 2008) se desarrolla el derecho fundamental al habeas data, regulando el manejo de datos personales desde el sector financiero. Luego, con la Ley 1273 (Congreso de la República de Colombia, 2009) se crea un bien jurídicamente tutelado "(…) *de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*" y finalmente, la Ley 1581 (Congreso de la República de Colombia, 2012) regula el manejo de datos de manera general, quiere decir que cualquier entidad que maneje un repositorio de datos debe ajustarse a esta reglamentación.

Como se enmarca, la legislación en Colombia ha tratado de ajustarse a los retos contemporáneos, sobre todo desde una perspectiva penal-sancionatoria, pero por la magnitud de este fenómeno tecnológico debe ir ajustándose más a la protección del derecho fundamental del habeas data y la dinámica de este sector, por lo que recientemente el Parlamento Europeo expidió el Reglamento (UE) 2016/679, cuyo marco normativo presenta innovación en el tema de responsabilidad en el tratamiento de datos de los responsables y encargados, reglamento que entró en vigencia en el primer trimestre del año 2018.

Por todo lo anterior, es que la óptica de estudio de este artículo científico girará en torno a la responsabilidad civil, cuyo objetivo principal es identificar la responsabilidad civil del manejo de datos en la era digital desde la perspectiva de la normativa jurídica colombiana y del marco normativo europeo, a partir del año 2012 hasta el año 2018, permitiendo desde el derecho comparado identificar qué aspectos el ordenamiento jurídico colombiano podría implementar en aras de proteger el derecho fundamental del habeas data, para lo cual se identificará la responsabilidad civil del manejo de datos en la era digital del marco normativo europeo dentro del periodo en mención; posteriormente se describirá la responsabilidad civil del manejo de datos en la era digital desde la normativa jurídica colombiana y, para finalizar, se establecerá similitudes y diferencias entre la normativa jurídica colombiana y el

marco normativo europeo frente a la responsabilidad civil del manejo de datos en la era digital a partir del año 2012 hasta el año 2018.

Este estudio se realiza partiendo de la base del concepto común de ambas legislaciones respecto a los datos personales, como "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, (...)"* (Parlamento Europeo & Consejo de la Unión Europea, 2016), es por ello que cuando hablamos de datos personales o habeas data se cruza una línea con otros derechos fundamentales como el derecho a la intimidad y buen nombre, cuya categoría constitucional les da el carácter de fundamentales, y toda lesión a la unidad de estudio "datos personales" lesiona estos derechos fundamentales conexos.

1. Materiales y métodos

La investigación aquí desarrollada es dentro del marco de la responsabilidad civil en el tratamiento de datos de la era digital, enfocada en la identificación y descripción del régimen de responsabilidad civil, cuyo objeto de estudio se inició para descubrir las falencias de nuestra legislación frente a las reglas jurídicas de una comunidad que ha sido pionera en temas de tecnología versus derechos humanos, como lo es la Unión Europea; se intentó describir el régimen de responsabilidad civil que cada una de estas jurisdicciones determina en el tratamiento de datos de la era digital, y posteriormente desde una perspectiva del derecho comparado identificar las similitudes y diferencias de ambos sistemas.

Este análisis comparativo lo realizamos tomando como base los avances más significativos para cada legislación, dando una temporalidad que inició en el año 2012 con la expedición de la Ley Estatutaria 1581 en Colombia, por la cual se dio desarrollo legislativo del habeas data, concluyendo nuestro estudio en el año 2018 con la entrada en vigencia del Reglamento Europeo sobre el tratamiento de datos personales y su libre circulación.

Por lo anteriormente mencionado la forma metodológica que se empleó en este artículo se estructuró en el tipo de investigación jurídica, con un enfoque comparativo entre la Unión Europea y Colombia, donde se caracterizaron las normas e instituciones jurídicas que desarrollan la protección y responsabilidad frente al habeas data, para lo que se aplicó un enfoque cualitativo analizando fuentes normativas, bibliográficas y jurisprudenciales de dichos países, y así mismo se

construyó el cuerpo del artículo con video exposición de autoridades en el tema y de textos científicos-jurídicos.

2. Fundamentación teórica

2.1. MARCO NORMATIVO EUROPEO (REGLAMENTO UE 2016/679)

Con la creación de las nuevas tecnologías el mercado acogió una dinámica para su distribución y expansión, viéndose obligado a adoptar el tratamiento de datos como elemento fundamental para el desarrollo de su actividad económica.

Esta dinámica impactó el concepto de derecho de datos personales, elevando su importancia hasta llegar a ser reconocido como un derecho fundamental, establecido así en la Carta de Derechos Fundamentales de la Unión Europea (año) en su artículo 8, y en el tratado de funcionamiento en el artículo 16.

Consiguiente a esto el parlamento europeo, el 27 de abril de 2016, expidió el Reglamento UE 2016/679 "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos" (Parlamento Europeo y Consejo de la Union Europea, 2016), estableciendo así principios y lineamientos jurídicos por los cuales se regirá el tratamiento de datos dentro de la Unión Europea.

Teniendo en cuenta lo anterior, en el artículo 5 del mencionado reglamento se implementaron unos principios que fundamentan y brindan lineamientos para la organización y estructuración del tratamiento de datos personales; a su vez estos principios se deben tener en cuenta para determinar la responsabilidad:

a) Principio de licitud, lealtad y transparencia, que se deberá implementar en la relación que establece el responsable en toda la cadena de recolección y tratamiento de datos respecto del interesado.

b) Limitación de la finalidad: en el proceso de recolección de datos personales el responsable debe establecer e informar al interesado sobre la finalidad del tratamiento de datos, y así mismo las acciones del responsable deben circunscribirse a lo que esté explícitamente acordado.

c) Minimización de datos: recapitulando el principio de limitación de la finalidad, el responsable debe establecer parámetros, garantizando que la recolección de los datos del interesado sean los pertinentes y estrictamente necesarios para cumplir la finalidad del tratamiento establecido.

d) Exactitud, relacionado con el principio de la minimización de datos: estos deben ser exactos y constantemente actualizados, permitiendo que el interesado pueda suprimir y rectificar datos que no corresponden a la realidad.

e) Limitación del plazo de conservación: el responsable, en concordancia con la finalidad del tratamiento de datos, debe establecer un tiempo de conservación necesario para el cumplimiento de esta.

f) Integridad y confidencialidad: el responsable debe garantizar al interesado una cadena de custodia pertinente y acorde con todos los estándares de seguridad establecidos evitando la pérdida, destrucción o daño a este derecho fundamental.

Por consiguiente, el Reglamento UE 2016/679 incluye el principio de responsabilidad proactiva como un elemento innovador dentro de la responsabilidad en el tratamiento de datos de la Unión Europea, donde se crea la necesidad para que el responsable aplique medidas técnicas y organizativas pertinentes a fin de garantizar y poder demostrar que el tratamiento es conforme al reglamento, por lo que se exige del responsable una actitud consciente, diligente y proactiva frente al tratamiento de datos. (AGENCIA ESPAÑOLA DE PROTECCION DE DATOS, 2019).

El concepto de responsabilidad proactiva, proviene del término inglés *Accountability*, que significa *"Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights"* (Presidencia de los Estados Unidos de América, 2012).

La cláusula de responsabilidad en el Reglamento Europeo se estableció en el artículo 24 de la siguiente manera:

Responsabilidad del responsable del tratamiento

> 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
>
> 2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. 3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento (Parlamento Europeo, Consejo de la Union Europea, 2016).

El artículo mencionado establece que la responsabilidad en el tratamiento de datos debe circunscribirse al establecimiento de "*medidas técnicas y organizativas por parte del responsable y encargado de los datos*"; estas deben ser apropiadas para garantizar y demostrar que el tratamiento de datos está acorde al Reglamento UE 679/2016; debe entenderse que esas medidas técnicas no se encuentran estandarizadas, puesto que las condiciones de la naturaleza, ámbito, contexto, fin del tratamiento, riesgos y gravedad para los derechos es variable, ya que su recolección es para fines diversos, por lo tanto deben ir encaminadas a proteger el derecho fundamental de datos personales.

La determinación de responsabilidad debe ser interpretada en concordancia con el principio de responsabilidad proactiva, infiriendo que del responsable y encargado del tratamiento se exige una actitud diligente, preventiva y activa respecto de la protección de datos, su tratamiento y efectividad en su utilización (Agencia Española de Proteccion de Datos, 2019).

La caracterización antes mencionada de la responsabilidad en el tratamiento de datos debe ser analizada desde la óptica del European group on tort law principles of european tort law (Principios de derecho europeo de la responsabilidad civil), específicamente en su capítulo 4 denominado "Responsabilidad por culpa", entendiéndose este tipo de responsabilidad de la siguiente manera:

> **Art. 4:101.** Una persona responde con base en la culpa por la violación intencional o negligente del estándar de conducta exigible.

> **Art. 4:102.** Estándar de conducta exigible:
>
> (1) El estándar de conducta exigible es el de una persona razonable que se halle en las mismas circunstancias y depende, en particular, de la naturaleza y el valor del interés protegido de que se trate, de la peligrosidad de la actividad, de la pericia exigible a la persona que la lleva a cabo, de la previsibilidad del daño, de la relación de proximidad o de especial confianza entre las personas implicadas, así como de la disponibilidad y del coste de las medidas de precaución y de los métodos alternativos.
>
> (…) (3) Al establecer el estándar de conducta requerido deben tenerse en cuenta las normas que prescriben o prohíben una determinada conducta.
>
> **Art. 4:103.** Deber de proteger a los demás de daños. Puede existir el deber de actuar positivamente para proteger a los demás de daños si así se establece legalmente, si quien actúa crea y controla una situación de peligro, si existe una especial relación entre las partes o si la gravedad del daño para una parte y la facilidad de evitarlo para la otra indican la existencia de tal deber (negrilla fuera de texto) (GRUPO EUROPEO SOBRE DERECHO DE DAÑOS, 2005).

Con este panorama se aclara la tipología de responsabilidad que se enmarca en esta actividad (tratamiento de datos), pues el artículo 24 del RGPD, al exigir una actitud diligente del responsable, nos pone *ad portas* de la responsabilidad subjetiva, cuyo elemento nuclear es la culpa, requisito determinante para imputar responsabilidad.

Según el PETL, que en su artículo 4:101 determina la responsabilidad por culpa como negligencia del estándar de la conducta exigible, este esquema propuesto tiene una indeterminación cuya adaptación debe hacerse a cada caso en concreto, pues es un modelo que se exige de un hombre razonable de cuya simplicidad debe tenerse presente otras variables como la pericia exigida en la actividad que realiza, y así mismo, el bien jurídicamente tutelado que protege, o las medidas de precaución respecto a daños previsibles.

Este concepto de responsabilidad por culpa nos determina un estándar que debe cumplir un sujeto responsable o encargado del tratamiento de datos, ya que tiene a su cuidado los derechos fundamentales de las personas que han otorgado su consentimiento para que este disponga de ellos. Más allá de esa confianza que deposita el usuario o interesado, está la responsabilidad de quien recibe esa confianza,

pues de su conocimiento y pericia se deriva esta relación que en principio es comercial, y cuyo trasfondo va más allá de adquirir un servicio.

Aunado a ello, en el artículo 4:202 del PETL se establece, desde la teoría organicista, que una persona que se dedica a una actividad empresarial y en la ejecución de su actividad los auxiliares o equipamientos técnicos causan por defecto un daño, la empresa será responsable del mismo, a menos que logre probar que se cumplió con el estándar de conducta exigible (Grupo Europeo sobre Derecho de Daños, 2005).

De esta cita se desprende otro punto importante a la hora de imputar la culpa y es: ¿Quién tiene la carga de probarla? Para este aspecto es importante aclarar que el tratamiento de datos es una actividad de carácter técnica, en la cual probar el daño derivado de la culpa o falta de diligencia o pericia es complejo, pues requiere de conocimientos especializados en la materia, por lo cual en el PETL (artículo 4:203) se habla de inversión de la carga de la prueba:

> (1) Puede invertirse la carga de la prueba de la culpa a la luz de la gravedad del peligro que la actividad en cuestión comporta.
>
> (2) La gravedad del peligro se determina de acuerdo con la gravedad del daño que en tales casos pueda producirse así como con la probabilidad de que tal daño llegue a suceder efectivamente (Grupo Europeo sobre Derecho de Daños, 2005).

Con esta reconstrucción normativa podemos inferir que la responsabilidad en el tratamiento de datos, a la luz del RGPD y PETL, se circunscribe a la responsabilidad subjetiva por culpa presunta:

> (…) incumplimiento de una obligación de medios da lugar a un régimen subjetivo de responsabilidad que puede ser con culpa probada –la carga de la prueba se encuentra en cabeza del demandante– o con culpa presunta –es al demandado a quien le compete probar en contrario– (Espinosa, 2007).

Por lo tanto, la víctima debe demostrar el daño o perjuicio que se le causó a su derecho fundamental, mientras el responsable o el encargado del tratamiento de datos debe desvirtuar la culpa, pues es quien tiene la pericia, conocimientos técnicos y acceso a la información para demostrar que actuó con diligencia, y que empleó las medidas técnicas y organizativas requeridas para la finalidad, naturaleza de datos y otros aspectos importantes al momento de determinar los medios de tratamiento y al momento de su ejecución.

2.2. Marco jurídico colombiano

Colombia, al ser establecido en la Constitución de 1991 como Estado social de derecho, realizó una consagración amplia de **Derechos Fundamentales,** entre los cuales se encuentra el artículo 15, que menciona lo siguiente:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...) (Asamblea Nacional Constituyente, 1991)

Este artículo es la consagración del derecho fundamental a la intimidad personal y al buen nombre, creando una obligación constitucional. Así mismo es garantía del tratamiento de datos desde su recolección y circulación, hasta la rectificación de los mismos.

Al considerarse el habeas data como derecho fundamental, sin que sobre él existiera alguna ley que lo reglamentara, la acción de tutela fue el mecanismo que permitió que se visibilizara logrando su protección y reconocimiento, lo que se evidencia con la postura que tuvo la Corte Constitucional (1993) en la Sentencia T-002, al determinar que en el tratamiento de datos económicos estaba inmerso un problema que afectaba directamente el derecho a la intimidad, procediendo así los presupuestos para interponer la acción de tutela.

Si bien en principio el derecho al habeas data fue considerado como un derecho conexo a la intimidad, se permitió por medio de la acción tutela que este derecho se fuera abriendo paso como derecho fundamental autónomo, y que su carácter de fundamental no dependiera exclusivamente del derecho a la intimidad.

Esta constitucionalización permite visualizar que la vulneración en el manejo de datos puede impactar directamente al derecho de la intimidad personal, familiar y al buen nombre, como lo manifestó la Corte Constitucional (1992):

> El habeas data, es el derecho de obtener información personal que se encuentre en archivos o bases de datos. Este derecho implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos. Con este derecho se pretende proteger la intimidad de las personas ante la creciente utilización de información personal por parte de la administración pública, de entidades financieras, educativas, profesionales u otras organizaciones privadas. Lo importante es que las personas no pierdan el control sobre la propia información, así como sobre su uso. Este derecho establece una doble línea de salvaguarda de los particulares; por una parte, incorpora obligaciones exigibles a entidades públicas y privadas que recopilan y tratan información, tales como de regirse por principios de lealtad, legitimidad con relación a la finalidad para lo que se recolectarán los datos. Y por otra parte, consiste en el derecho que tiene toda persona a exigir del Estado el respeto a derechos como el de la intimidad personal y familiar y a su buen nombre (Sentencia T-444).

Con base en lo anterior, podemos establecer que la Corte habla de una doble línea, en el entendido que las entidades y el Estado, al manipular nuestros datos, debe proteger el derecho a la intimidad personal familiar y buen nombre, y el derecho al habeas, ambos amparados por nuestra Carta Política de 1991.

La caracterización de "doble vía" que expresa la Corte Constitucional (1995) sobre el derecho del hábeas data, ocasionó que, más allá de ser un conducto para la protección de la intimidad, fuera considerado como derecho autónomo, identificación que se dio en la Sentencia SU-082, al determinar que el núcleo esencial del habeas data está integrado por el derecho a la autodeterminación informática y libertad en general, y en especial económica.

El elemento de la autodeterminación informática se describe como la facultad que tiene la persona para autorizar la conservación, uso y circulación de sus datos personales, de acuerdo con las regulaciones legales; por otro lado, la libertad económica podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no hayan sido autorizados por la persona concernida o por la ley (Corte Constitucional, 1995).

Dentro de esa línea jurisprudencial, la Corte Constitucional (2013) hace la siguiente afirmación:

> Para la Corte, el habeas data es un derecho de doble naturaleza. Por una parte, goza del reconocimiento constitucional de derecho autónomo, consagrado en el artículo 15 de la Constitución y, por otra, ha sido considerado como una garantía de otros derechos. Como derecho autónomo, tiene el habeas data un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quién (y cómo) administra la información que le concierne y el poder de su titular de conocer, actualizar, rectificar, autorizar, incluir y excluir información personal cuando ésta sea objeto de administración en una base de datos (Sentencia T-058).

De esta caracterización como derecho fundamental autónomo deben establecerse pautas cuya ejecución estén dentro del marco del respeto y la garantía de la protección al habeas data, no solo por ser un derecho fundamental en sí mismo, sino por ser garantía de otros derechos, como bien lo manifiesta la Corte.

Por lo anterior, el cuerpo legislativo ha expedido la Ley Estatuaria 1581 de 2012, que regula este derecho fundamental determinando unas condiciones mínimas para que el tratamiento de los datos, principalmente los "datos personales" se realice de manera legítima y acorde con el artículo 15 constitucional.

En el artículo 4º de la ley antes mencionada se establecen los "*principios para el tratamiento de datos personales",* de la siguiente manera*:*

El principio de legalidad determina que todo tratamiento de datos debe ajustarse a la Ley 1581 de 2012 y las reglamentaciones de dicha actividad.

La finalidad de la actividad en cuestión debe ser legítima y de acuerdo con los parámetros establecidos en la Constitución y la ley.

El tratamiento de datos tiene un carácter de libertad para el titular de los datos, pues es quien autoriza al responsable por medio de un consentimiento previo, expreso e informado sobre la actividad que se va a realizar con la información suministrada.

La información que suministra el titular debe ser tratada bajo el principio de veracidad o calidad, donde el responsable debe garantizar que la información sea completa, exacta, actualizada, comprensible y comprobable.

El responsable del tratamiento debe suministrar información sobre los mismos al titular de los datos en cualquier momento.

El principio de acceso y circulación restringida establece que los datos suministrados solo pueden ser manipulados por personas o entidades autorizadas por el titular de los mismos, no solo en su acceso y tratamiento, sino en su tráfico.

Dentro del tratamiento se establece un régimen de seguridad que debe garantizar el responsable del tratamiento de datos para evitar alguna afectación al habeas data, empleando técnicas humanas y administrativas necesarias.

El principio de confidencialidad obliga a todas las personas que se involucren en el tratamiento de datos personales a preservar la información que a ellos sea suministrada durante y después de la ejecución de las actividades que inicialmente se establecieron.

En los artículos 17 y 18 de la Ley 1581 de 2012 se establecen los deberes de los responsables y encargados del tratamiento de datos, presentándose una concurrencia de obligaciones entre estos sujetos, como es el caso del literal a en ambos artículos, que dice "*a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data".*

Al respecto, la Corte Constitucional (2011), en Sentencia C-748 ha manifestado que estos sujetos tienen una responsabilidad concurrente frente a la veracidad, integridad, finalidad e incorporación del dato, teniendo en cuenta que la recolección y procesamiento de estos no es una actividad neutra que impida al encargado del tratamiento responder, pues a este le concierne garantizar que se cumplan los requisitos para que un dato personal pueda ser objeto de tratamiento; en igual sentido, el Alto Tribunal constitucional señala que si no se puede identificar la posición de los sujetos (responsable y encargado), estos responderán de forma solidaria y no podrán excusar sus deberes de actualización, rectificación y exclusión, o supresión del dato.

Con lo anterior tenemos que, si bien en ambos artículos se determinan unas obligaciones que en principio son taxativas, con la estipulada en el literal A de ambos artículos genera una extensión de responsabilidad dentro de todo el ejercicio del tratamiento de datos, por ello la Corte Constitucional (2011), en la Sentencia C-748 realiza una interpretación de la actitud del juzgador al momento de garantizar la protección al habeas data, aludiendo que corresponde a las autoridades judiciales garantizar al titular del dato la protección que exige el ejercicio de su derecho, sin quedar sujeto a limitaciones que se deriven de la exclusión de la responsabilidad frente a los deberes legales de los sujetos pasivos involucrados en el tratamiento de datos, en el entendido que las obligaciones establecidas en la ley no son taxativas

sino enunciativas, pues los responsables y encargados del tratamiento tendrán otros deberes emanados del derecho al habeas data, concernientes a los beneficios que otorga el mismo para sus titulares.

Por consiguiente, la obligación y compromiso del responsable y el encargado del tratamiento de datos tiene una cobertura amplia y solidaria, en procura de que el titular del habeas data tenga posibilidad de exigir la protección a su derecho sin tener que especificar a quién endilgar responsabilidad entre los sujetos activos de la cadena del tratamiento de datos.

La Ley 1581 de 2012 es regulada por el Decreto 1377 de 2013, expedido por el Presidente de la República de Colombia, decreto que incluyó el principio de responsabilidad en el artículo 26, determinando que los responsables del tratamiento de datos ante cualquier requerimiento de la Superintendencia de Industria y Comercio deben demostrar que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012, para lo cual la autoridad debe analizar desde la proporcionalidad las siguientes variantes: naturaleza jurídica del responsable, naturaleza de los datos personales, tipo de tratamiento y riesgos potenciales.

Adicionalmente, el artículo subsiguiente (27) de este decreto determina que los responsables deben adoptar políticas internas efectivas y apropiadas para el tratamiento de datos personales, acudiendo a los requerimientos de la Superintendencia de Industria y Comercio.

Por lo anterior e innovador que resultó para el régimen de tratamiento de datos la adopción del principio de responsabilidad, denominado "Responsabilidad demostrada", la Superintendencia de Industria y Comercio (2015) expidió un manual para la implementación de este principio; como primera medida resalta la necesidad de que los sujetos obligados en el tratamiento de datos implementen un "*Programa integral de la gestión de datos"* que corresponde a un proceso de debida diligencia que se desarrolla en la organización, en el cual se incorporen políticas que respondan a ciclos internos de gestión de datos, y este genere resultados que permita probar un grado de diligencia especial.

Adicionalmente la SIC (2015) afirma que con la permanencia del programa integral de gestión de datos personales se garantiza su eficacia, el cumplimiento y la adherencia a estándares de Responsabilidad Demostrada.

Finalmente, la SIC (2015) menciona que este principio de responsabilidad demostrada no es solo frente a la autoridad administrativa, sino ante el titular de los datos personales.

Posteriormente en Colombia, con el Decreto 1413 (Ministerio de las TIC, 2017), se adopta una medida dentro de la responsabilidad proactiva denominada "la privacidad desde el diseño y por defecto", las cuales, más que medidas, se convirtieron en principios dentro del tratamiento de datos (Remolina A. & Álvarez Z., 2018). Este principio se estableció en el numeral 6 del artículo 2.2.17.1.5 del decreto mencionado, ya que busca que se adopten medidas preventivas con anterioridad a la recolección de datos y durante el tratamiento de los mismos, con el fin de evitar vulneración al derecho a la privacidad o confidencialidad, exigiendo así un proceso de gestión de información preestablecido (Presidencia de la República de Colombia, 2017).

Con lo anterior tenemos que en Colombia desde el año 2013 el régimen de responsabilidad en el tratamiento de datos se desarrolla bajo el Principio de Responsabilidad Demostrada, término que proviene del inglés "*accountability*", que significa responsabilidad, y en el mundo del tratamiento de datos se refiere a la manera que una organización acata en la práctica las regulaciones realizadas sobre la materia, y así mismo logra demostrar que lo ejecutado es útil, pertinente y eficiente (Remolina A. & Álvarez Z., 2018).

Ahora bien, enfocándonos en el objeto de estudio, encontramos que el Principio de Responsabilidad Demostrada se enmarca en la tipología de la responsabilidad subjetiva, al consagrar que el responsable debe establecer un *Programa Integral de la Gestión de Datos* cuya finalidad es alcanzar una debida diligencia en su actividad, afirmación que nos sitúa en el campo de la responsabilidad subjetiva, dentro de la cual aparece el elemento de culpa que en principio debe ser acreditado por el demandante pero, según el Principio de Responsabilidad Demostrada, es el responsable o encargado del tratamiento de datos quien debe desvirtuarla y demostrar que su actuación estuvo ajustada a la Ley 1581 de 2012, al Decreto 1377 de 2013, y a cualquier otra reglamentación de la SIC, por ello se determina como culpa presunta, por la inversión de la carga de la prueba.

Frente a esto la abogada Salazar H. (2013), en un artículo de la revista de la Universidad del Externado manifiesta que el solo hecho de vulnerar una disposición legal es la prueba en sí misma de la culpa.

Continuando con el mismo artículo, Salazar H. (2013, citando a Arturo Alessandri Rodríguez, 1981, pp. 175-177), afirma y cita:

> La apreciación de la conducta del autor del daño es innecesaria si éste proviene de la violación de una obligación determinada impuesta por la Ley o un reglamento, si hay lo que alguno denominan culpa contra la legalidad.
>
> (…) Cuando así ocurre, hay culpa por el solo hecho de que el agente haya ejecutado el acto prohibido o no haya realizado el ordenado por la Ley o el reglamento, pues ello significa que omitió las medidas de prudencia o precaución que una u otro estimaron necesarias para evitar un daño.
>
> Este criterio ha sido acogido por la doctrina nacional que al respecto ha afirmado:
>
> El ordenamiento jurídico impone a todos los individuos, en forma expresa y taxativa, unos determinados comportamientos. En tales circunstancias, el incumplimiento de cualquiera de esos deberes u obligaciones, ipso facto genera una culpa en cabeza del transgresor de la norma
>
> De acuerdo con lo expuesto, comparto la posición de quien indica que la prueba de la infracción "ya lleva ínsita la demostración de la culpa, por lo que un doble requerimiento de este elemento podría resultar excesivo" (Ortiz Baquero, 2011: 209). Lo anterior es así, además, porque tal circunstancia, la violación de una norma imperativa, corresponde al concepto tradicional de culpa, según el cual "hay culpa cuando no se obra como se debiere, cuando no se hace lo que hubiera debido hacerse" (Alessandri Rodríguez, 1981: 172) (p. 158).

Esta postura se ratifica con lo mencionado por la SIC (2019) en la Resolución 4086:

> El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre el tratamiento de datos sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que *los* administradores de las organizaciones sean proactivos respecto del tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar los derechos de los titulares de los datos personales y su gestión siempre sea respetuosa de los derechos humanos.
>
> (…) Considera el despacho, que estando demostrado que si bien la sociedad estuvo presta a garantizar el derecho del titular de suprimir sus datos, se

> infringió el deber que tienen los responsables de la información establecido en el literal g) artículo 17 la ley 1581 de 2012, puesto que no acreditó unos procedimientos y buenas practicas establecidos (…) (SIC, 2019, p. 13).

En conclusión, el régimen de responsabilidad en el tratamiento de datos aplica el principio anglosajón de la responsabilidad demostrada, donde la culpa se presume del responsable del tratamiento de datos, y al titular afectado le corresponde probar los elementos de responsabilidad exceptuando la culpa, pues con el solo hecho de que el responsable vulnere una norma queda probada en sí misma la culpa, ya le toca al responsable desvirtuarla.

3. Resultados y hallazgos

El reconocimiento como derecho fundamental al habeas data en la Unión Europea tuvo su impacto por la implementación de nuevas técnicas en el mercado; por su parte, en Colombia el reconocimiento de este derecho se derivó del derecho a la intimidad, consagrado en la Constitución de 1991 como un derecho fundamental, cuyo debate jurídico permitió caracterizar al habeas data como un derecho autónomo, establecido así por la Corte Constitucional en el año 1995, de lo cual se infiere que en ambas legislaciones, al denominar el derecho del habeas data como derecho fundamental, exige una protección especial por parte del Estado y sus entes de control para garantizar a los individuos su efectiva protección.

Por tal motivo, la protección en la actualidad del derecho al habeas data presenta un discusión jurídica, pues se ha evidenciado que los agentes externos tecnológicos como redes sociales, artefactos tecnológicos, plataformas de entretenimiento, entre otras, llegan a impactar negativamente este derecho fundamental, presentando una vulneración del mismo, por lo que se está evidenciado la necesidad que las áreas de la tecnología y del derecho determinen una regulación de aquella, en el entendido que el desarrollo de las plataformas y artefactos debe respetar unos estándares mínimos de derechos fundamentales.

La Unión Europea en su reglamento busca la regulación normativa del derecho fundamental del habeas data, y la determinación de la responsabilidad de los encargados y el responsable del tratamiento de datos con la implementación de principios y lineamientos jurídicos; por otra parte, el cuerpo normativo colombiano estableció una serie de principios para que el tratamiento de datos se realice de manera legítima y acorde al artículo 15 de su Carta Política (1991).

De lo anterior se identifica una ausencia de regulación respecto al régimen de responsabilidad en la Ley Estatutaria 1581 de 2012 de Colombia, que posteriormente

fue complementada con la expedición del Decreto Reglamentario 1377 de 2013, en el cual se incluyó el régimen de responsabilidad en el tratamiento de este derecho fundamental y se subsanó aquel vacío.

Otro aspecto de este ejercicio comparativo fue sobre el principio de plazo de conservación, donde la legislación europea lo establece como la obligación que tienen los encargados y responsables de conservar los datos hasta el cumplimiento de la finalidad del tratamiento, mientras que en la ley estatutaria colombiana existe un principio de confidencialidad, en el entendido de que todos los sujetos que se vean involucrados con el tratamiento de datos pueden preservar la información durante y después de la ejecución de las actividades acordadas, mientras se esté dando cumplimiento a la confidencialidad.

Con lo anterior se evidencia que la legislación colombiana presenta una incongruencia en sus principios, ya que la mayoría tiene como finalidad la protección al derecho fundamental del habeas data, pero con el principio de confidencialidad desnaturaliza su objetivo, permitiendo que los encargados del tratamiento de datos puedan conservarlos después de realizar las actividades acordadas, posibilitando la filtración y utilización indebida de los mismos.

Ahora bien, frente al régimen de responsabilidad en el tratamiento de datos se establece que ambas legislaciones buscan del responsable y encargado una actitud de debida diligencia que permita evitar cualquier vulneración o alteración a los datos que son suministrados por los titulares; para lograr este objetivo en el reglamento de la Unión Europea se estableció el principio de responsabilidad proactiva, el cual busca que el responsable adopte medidas técnicas y organizativas creando en este una actitud consciente, diligente y proactiva.

Por su parte la legislación colombiana estableció el principio de responsabilidad demostrada, que busca implementar técnicas humanas y administrativas para que estas le permitan demostrar al encargado o responsable su diligencia cuando sea requerido por alguna autoridad, o se le endilgue responsabilidad alguna.

De lo anterior se logra identificar que el régimen de responsabilidad adoptado por ambas legislaciones tiene aspectos y fines similares, pues exigen una actitud diligente y preventiva por parte de los encargados del manejo de datos, caracterización con la cual nos enmarcamos en una responsabilidad subjetiva con culpa presunta, pues la carga de la prueba está en manos de los responsables del tratamiento de datos, ya que estos son los que tienen la pericia, medios y acceso directo e inmediato a la información para desvirtuar la responsabilidad.

De la lectura de las normas de ambas jurisdicciones se infiere la caracterización de la responsabilidad como solidaria, determinación que las dos legislaciones comparten no solo en su enunciación, sino en su finalidad, pues buscan la protección de la parte más débil de esa relación, quien es el titular de los datos, y con ello se logra determinar que la responsabilidad está en cabeza del responsable y encargado del tratamiento de datos, que por más que se delimiten sus tareas, a la hora de imputar responsabilidad el sujeto que interpone la acción no debe individualizar la responsabilidad, sino que la dirige contra ambos, esto con el fin de que sus pretensiones no sean desconocidas por ausencia o error en la identificación de los sujetos pasivos.

Finalmente se evidencia que el mundo jurídico está volcando su análisis y estudio sobre aquellos retos que los avances tecnológicos nos presentan, y que a su vez su desarrollo acelerado sin limitación llega a vulnerar derechos fundamentales, por ello la regulación del tratamiento de datos personales en el mundo de la información requiere un estudio profundo, donde la imputación de responsabilidad se convierte en una herramienta de prevención del daño, siendo coherente con la principialística que ambas legislaciones nos presentan.

Conclusiones

Con el estudio realizado a la legislación de la Unión Europea y Colombia, en relación con el régimen del tratamiento de datos personales, se logró identificar que los fines y la responsabilidad implementada en ambos sistemas jurídicos son similares.

Desde el punto de vista de la finalidad, las legislaciones objeto de estudio buscan prevenir un daño a los datos personales, exigiendo a los responsables y encargados la obligación de implementar medidas técnicas, organizativas, humanas y administrativas que garanticen dicho fin, con lo se tiene que el objetivo de esta finalidad no se cumple, ya que siempre que se emprenden acciones estas se dan por una afectación al derecho fundamental; la prevención insignia de este modelo debe estar acompañada de una vigilancia y control activo y permanente de la autoridades administrativas y entes de control hacia los sujetos que tratan datos personales, para que toda posible afectación sea evitada y no se concrete en un daño hacia el titular.

Finalmente, desde la responsabilidad tenemos que el régimen implementado en la legislación de la Unión Europea y Colombia, partiendo de los principios de responsabilidad proactiva y responsabilidad demostrada, se identifica que este régimen se estructura sobre la responsabilidad subjetiva para imputar responsabilidad, pues en ambas lo que se busca es que el responsable o encargo del

tratamiento de datos mantenga una actitud de debida diligencia, aspecto fundamental para poder endilgar responsabilidad con culpa; con ello, al momento de imputar responsabilidad, el responsable del tratamiento de datos debe desvirtuar la culpa probando su diligencia y cuidado en la implementación de las técnicas preventivas que sean acordes con los datos recolectados y la finalidad del tratamiento.

En conclusión, se identifica que el régimen de responsabilidad para ambas legislaciones en el tratamiento de datos es la responsabilidad subjetiva con culpa presunta.

Bibliografía

Agencia Española de Proteccion de Datos (s.f.). *Principios*. Madrid, España. Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

Asamblea Nacional Constituyente (1991). *Constitución Política de Colombia*. Bogotá: Imprenta Nacional.

Congreso de la República de Colombia (2009). Ley 1273. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Bogotá: Imprenta Nacional.

Corte Constitucional (1992). Sentencia T-444. M.P.: Alejandro Martínez Caballero. Bogotá, Colombia.

Corte Constitucional (1995), Sentencia SU-082. M.P.: Jorge Arango Mejia. Bogotá, Colombia.

Corte Constitucional (2013). Sentencia T-058. M.P.: Alexei Julio Estrada. Bogotá, Colombia.

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

Corte Constitucional (1993). Sentencia T-002. M.P.: Alejandro Martínez Caballero. Bogotá, Colombia.

Espinosa, F.M. (2007). "Título del artículo". En: *Revista de Opinion Jurídica Scielo.* Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302007000100008

Gayo, M.R. (2017). "Big data: hacia la protección de datos personales basada en una transparencia y realidad aumentadas". En: *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*. N° 7. Ciudad: Bogotá. Editorial: Universidad de los Andes.

Grupo Europeo sobre Derecho de Daños (2005). *Principios de derecho europeo de la responsabilidad civil.* Disponible en: http://civil.udg.edu/php/biblioteca/items/298/PETLSpanish.pdf

Parlamento Europeo & Consejo de la Unión Europea (2016). Reglamento (UE) 2016/679. *Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)*. Unión Europea .

Parlamento Europeo Consejo de la Union Europea (2016). Reglamento UE 2016/ 679. 47. Ciudad.Bruselas.

Powerdata (s.f.). *Centro de recursos.* Disponible en: https://www.powerdata.es/big-data

Presidencia de la República de Colombia, (2013). Decreto 1377. Bogotá: Imprenta Nacional.

Presidencia de la República de Colombia (2017). Decreto 1413. *"Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*. Bogotá: Imprenta Nacional.

Presidencia de los Estados Unidos de America (2012). *Consmer Data Privacy In A Networked World.* Washington: The White House.

Remolina A., N. & Alvarez Z., L.F. (2018). *Guía GECTI para la implementación del principio.* Bogotá: Universidad de los Andes .

Salazar H., C. (2013). "Algunos apuntes sobre la culpa en la responsabilidad derivada de las prácticas comerciales restrictivas de la competencia". En: *Revista Digital de Derecho Administrativo*. N° 10 (147-160). Ciudad:Bogotá. Editorial: Universidad Externado de Colombia.

Superintendencia de Industria y Comercio (2019). Resolución 4086. Bogotá: Imprenta Nacional.

Superintendencia de Industria y Comercio (2015). *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability).* Bogotá.