# PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA FRENTE AL *PROFILING* Y ENTORNOS DIGITALES

YAHAIRA ARÉVALO ARAGÓN



UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
VILLAVICENCIO
2020

# PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA FRENTE AL *PROFILING* Y ENTORNOS DIGITALES

YAHAIRA ARÉVALO ARAGÓN

Trabajo de grado presentado como requisito para optar para el título Abogada

Director
Mg. RODRIGO CORTES BORRERO
Magíster en Derecho Contractual Público y Privado
Doctorando en Derecho Privado

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
VILLAVICENCIO
2020

**Autoridades Académicas**

**P. José Gabriel MESA ANGULO, O. P.**
Rector General

**P. Eduardo GONZÁLEZ GIL, O. P.**
Vicerrector Académico General

**P. José Antonio BALAGUERA CEPEDA O.P.**
Rector Sede Villavicencio

**P. Rodrigo GARCÍA JARA, O.P.**
Vicerrector Académico Sede Villavicencio

**Adm. JULIETH ANDREA SIERRA TOBÓN**
Secretaria de División Sede Villavicencio

**PhD. SONIA PATRICIA CORTES ZAMBRANO**
Decana Facultad de Derecho

**Contenido**

**Pág.**

## Lista de Tablas

**Pág.**

## Lista de Figuras

**Pág.**

## Lista de Anexos

**Pág.**

## Resumen

La explotación de los datos personales de los usuarios en el entorno digital, se ha denominado la nueva moneda del siglo XXI, generando un impacto sobre el enfoque que deben tener los ordenamientos jurídicos de los Estados para lograr un nivel adecuado para la protección de datos personales (PDP) durante tratamientos de datos personales (TDP) como lo es la actividad de *profiling*. Este escrito monográfico es un estudio socio-jurídico, basado en un análisis normativo, sobre el impacto que tiene el TDP en el derecho al habeas data, y la respuesta de la legislación colombiana para conseguir un adecuado nivel de PDP acorde con los estándares supranacionales.

A su vez, se aborda el estudio de los mecanismos de PDP en Colombia, entre ellos el principio de responsabilidad demostrada, a cargo de la vigilancia de la Superintendencia de Industria y Comercio mediante la Delegatura de Protección de Datos Personales (DPDP), como medios para alcanzar el nivel adecuado de PDP en el entorno digital.

**Palabras clave:** perfilado de datos - datos personales - habeas data - responsabilidad demostrada- inteligencia artificial - tratamiento de datos personales.

## Abstract

The exploitation of users' personal data in the digital environment has been called the new currency of the 21st century, generating an impact on the approach that the legal systems of the States must have to guarantee an adequate level of protection of personal data during processing of personal data such as profiling. This monograph is a socio-legal study, based on a normative analysis, on the impact that personal data processing has on the right to habeas data, and the response of Colombian law to achieve an adequate level of protection of personal data.

At the same time, the mechanisms for the protection of personal data were studied, including the principle of demonstrated responsibility, under the supervision of the Superintendence of Industry and Commerce through the Office for the Protection of Personal Data, as means to achieve the appropriate level of personal data protection in the digital environment.

**Keywords:** data profiling - personal data - habeas data – accountability - artificial intelligence - processing of personal data.

# Introducción

Los datos personales como la nueva moneda digital (Citado por Remolina, 2010, p. 492), potencializan y mejora la capacidad de las empresas para diagnosticar qué y cómo ofrecer al usuario productos y servicios a partir de sus intereses, gustos, creencias o incluso sus emociones y decisiones.

El rápido desarrollo de la tecnología y en especial, de la Inteligencia artificial, obliga al derecho a dar pasos contiguos y sólidos para dar respuesta a los retos impuestos por la sociedad digital (Garrell, Guirela, 2010; Polo, 2020) - el homo digitalis (Terceiro, 1996), entre ellos, el perfilado de datos personales o *profiling* (Helbet, 2016; Martinez, 2019), es la práctica que surge como respuesta a la necesidad de las empresas de identificar, analizar y potenciar el uso de los intereses de los usuarios a partir de los datos personales que son compartidos en los diferentes entornos digitales como redes sociales, Marketplace, internet, entre otros. Esta realidad, lleva a cuestionar cuál es el riesgo de vulneración de derechos como el habeas data al implicar la constante digitalización de la privacidad.

Los recientes casos que han puesto en entre dicho las practicas adecuadas y legales de los datos personales en el entorno digital, son una pequeña muestra de los retos que debe enfrentar el derecho. Ejemplo de ello es el sonado caso *Cambridge Analitycs* que envolvió a la empresa Facebook en una investigación por la supuesta venta de datos personales para ser tratados con fines políticos, o en el 2015 cuando el IA de *Google Photos* confunde a personas afrodescendientes con fotos de gorilas, y aún más reciente, la polémica por las declaraciones emitidas por el presidente estadounidense Donal Trump, que busca prohibir la empresa China *Tik Tok*, por considerarla una amenaza para la seguridad de la nación y los datos personales de los ciudadanos al ser un medio de espionaje (El Tiempo, 2020).

Así, la posibilidad de afectación al derecho de habeas data es latente en el entorno digital, requiere ser analizada. El entorno digital es amplio, dúctil, de rápido desarrollo y poco trasparente es necesario estudiar los grandes avances de la tecnología para advertir a la comunidad sobre estas

prácticas y su papel para la protección de sus derechos, quienes constantemente se ven envueltos en la paradoja de la privacidad (Chen & Wen, 2019; Point Zero Production Inc, 2020), al compartir sus datos, el usuario puede entender el riesgo que esto representa para sus datos personales pero igual, sucumben a las políticas de tratamiento de datos abusivas, ejemplo de ello es el reciente fallo del tribunal alemán que condenó a la empresa Facebook por la implementación de cláusulas abusivas en sus contratos (Bundesgerichtshofs, 2020), lo que genera una afectación en la autodeterminación informática (Corte Constitucional, Sentencia T-729, 2002). Más aun en el actual aumento de actividad en el entorno digital con ocasión de la Pandemia del año 2020.

Por lo tanto, se planteó como problema de investigación ¿Cuál es el estado actual de protección de los datos personales en el ordenamiento jurídico colombiano dentro del entorno digital (redes sociales y plataformas de e-commerce) y qué desafíos principales presenta este sector?

Determinando el estado actual de la protección a los datos personales en el entorno digital, a través de la identificación de las normas nacionales y supranacionales aplicables, los mecanismos para la protección de datos personales y los desafíos que enfrenta el derecho colombiano para tener un nivel adecuado de protección de datos personales.

Por consiguiente, este escrito se realizó sobre el estudio a los riesgos del entrono digital y el estudio de las disposiciones nacionales y supranacionales, los mecanismos de protección de datos personales en Colombia y el principio *Accountability*. Usando una metodología cualitativa de tipo socio jurídico con un enfoque normativo y jurídico-descriptivo. De igual forma, se analizó la respuesta dada por la Superintendencia de Industria y Comercio a través de la Dirección de Investigación para la Protección de datos personales (DIPDP), que resolvió los cuestionamientos planteados, acerca de la PDP en el entorno digital, dentro del derecho de petición dirigido a la DIPDP.

# Objetivos

## Objetivo general

Determinar el estado actual de protección a los datos personales en el entorno digital (redes sociales y plataformas de e-commerce) en Colombia.

## Objetivos específicos

- Describir las nociones previas y el estado actual normativo de la protección de los datos personales en Colombia.
- Especificar cómo se protegen los datos personales en el entorno digital (redes sociales y plataformas de e-commerce)
- Analizar los desafíos de la protección de los datos personales en el entorno digital. (Profiling- ventas de datos-IA- Apps)

# 1. Marco referencial

## 1.1. Marco Conceptual

### 1.1.1. ¿Qué es un Dato Personal?

El término de dato personal incluye la noción de información y la noción de dato armonizada con el ámbito de la persona natural. Esto quiere decir que, la persona ostenta cualidades o características que la identifican y permiten la obtención de información; por ello, los datos personales son atribuibles solo a personas naturales. De manera genérica, el dato contiene información acerca de una persona u objeto que pueda ser susceptible de tener un contenido informativo, el cual puede ser expresado para ser adoptado y servir de ayuda generalmente para hacer mayor o menor identificable algo. Es decir que, los datos ofrecen información sobre un ente o ser que tiene por objetivo su identificación. Según Elías, citado por Delon (2019) "el dato es la representación de una porción de la realidad" (Delon, 2019, p. 3).

A su vez, la ley 1581 de 2012 regula de manera general la protección de datos personales y habeas data en Colombia, define el dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (Ley 1581, 2012, art. 3)

Ahora bien, partiendo de la premisa que un dato contiene información general o específica sobre algo o alguien que expresa su realidad. En el caso de los datos que están relacionados con el ámbito propio de la persona, se presenta como la realidad representada a través de información que accede a la identificación de una persona a partir de sus características de contenido morfológicas, psicológicas, intrínsecas o extrínsecas; dependiendo del tipo de dato personal al que se haga referencia o, como bien lo señala Galvis, dato personal es "todo tipo de información vinculada a una persona y que permite llegar a ella" (Galvis, 2018, p. 134). Los datos personales cobran especial importancia al tocar derechos fundamentales como la privacidad o la intimidad de la persona, aún más en la actualidad, los datos personales son considerados como lo señala Kuneva,

citado por Remolina, “el nuevo petróleo de la internet y la nueva moneda del mundo digital” (Remolina, 2010, p. 492).

### 1.1.2. Tipos de datos

Una vez expuesta la noción de dato personal, resulta pertinente identificar los tipos de datos, particularmente aquellos que se derivan de los datos personales. Un dato personal puede abarcar desde la información que identifica una persona según su lugar de nacimiento, las características físicas, psicológicas, gustos e intereses, hasta las decisiones que toma una persona en el entorno digital. Lo primero a establecer es que, se presentan tantos tipos de datos personales como ámbitos de una persona. Así, de manera genérica se puede establecer datos personales intrínsecos, extrínsecos, según si corresponden a expresiones externas o internas que identifica a una persona, datos biométricos, datos morfológicos, datos psicológicos, datos religiosos, datos políticos, entre otros. Gozaíni, citado por Delon (2019), identifica otra categoría denominada “datos personales no existenciales” (p.4) en esta categoría se incluye aquella información que se obtiene a partir de las decisiones que toma una persona a lo largo de su vida y que la identifican con cualquier categoría establecida siempre y cuando sea el resultado de su elección (Delon, 2019, p. 4).

En Colombia, de acuerdo con la ley 1266 de 2008 y la jurisprudencia nacional, los tipos de datos son:

- Dato privado, debido a su naturaleza íntima o reservada solo es relevante para el titular.
- Dato semiprivado, difiere del dato reservado, íntimo o público, aquel relevante para el titular o un grupo determinado.
- Dato público, el que así lo define la ley o la constitución.
- Dato sensible, aquel que afecta la intimidad del titular, lo que puede generar discriminación.

  (Superintendencia de Industria y Comercio (SIC), 2020, p.1).

En cuanto a los datos sensibles, están estrechamente relacionados con el derecho fundamental a la intimidad puesto que, debido a su contenido, es decir a la información que trasmiten de una persona, gozan de especial protección por corresponder al ámbito más íntimo de la persona, por ello su trascendencia. Según la jurisprudencia constitucional los datos sensibles

“afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación” (Corte Constitucional, Sentencia T-114, 2018)

Resulta importante mencionar una categoría especializada por el objetivo que cumpliría, se propone la categoría de los datos personales sensibilizados, correspondiente a aquellos que si bien pueden pertenecer a una u otra de las categorías mencionadas anteriormente; al ingresar en un contexto de alto TDP se “recategorizan” con el fin de brindar una protección especial al encontrarse en un espacio de peligro por ser tratados bajo posible indiscriminación y a los cuales se debe asegurar la autonomía y decisión de la persona que los proporciona. Así, una posible definición de datos personales sensibilizados es aquellos datos que pertenecen a una persona por permitir su identificación, y que son compartidos en un contexto digital de alto TDP que requiere de especial protección legal por afectar principios y derechos que afectan a la persona.

### 1.1.3. Superintendencia de Industria y Comercio (SIC)

La Superintendencia de Industria y Comercio (SIC), es el ente de vigilancia y control colombiano encargado de regular las relaciones surgidas entre las actividades comerciales bajo la especial protección de los derechos de los consumidores. Es una agencia estatal que regula la competencia comercial en el territorio colombiano. Se creó en el año 1968 mediante el Decreto 2974 del 03 de diciembre de 1968. La SIC está conformada por las siguientes delegaturas para el desarrollo de sus funciones:

- Delegatura de propiedad intelectual.
- Delegatura Protección al Consumidor.
- Delegatura para el Control y Verificación de Reglamentos Técnicos y Metrología legal.
- Delegatura para la Protección de la Competencia.
- Delegatura para Asuntos Jurisdiccionales.
- Delegatura para la Protección de Datos Personales.

#### *1.1.3.1. Delegatura para la protección de datos personales.*

Teniendo en cuenta que la SIC cuenta con varias dependencias que se encargan de las diferentes funciones y la regulación de la competencia comercial en el territorio colombiano; respecto a la protección de Habeas Data se encuentra la Delegatura para la Protección de Datos Personales que, es el resultado de la entrada en vigencia de la Ley 1581 de 2012, como la expresión de la obligación y función legal de la SIC de proteger el Habeas Data, así, el artículo 19 señala que "la Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley" (Ley 1591, 2012, art. 19).

Igualmente, es la encargada de vigilar y regular los procedimientos consagrados en la ley 1266 de 2008, sobre todo cuando se trata de datos personales (SIC, 2020b). La Delegatura para la Protección de Datos Personales resalta entre sus funciones procurar el cumplimiento de la normatividad en materia de protección de datos personales, adelantar investigaciones cuando se esté ante una posible vulneración sobre el TDP y ordenar medidas dirigidas a fomentar la protección de los datos personales (Decreto 4886 de 2011, art. 16).

### 1.1.4. Comercio Electrónico

El comercio electrónico, supone en principio un ámbito digital o virtual en el cual se llevan a cabo todo tipo de relaciones comerciales. Es el resultado de la rápida expansión de internet, el acceso cada vez más posible y, además, la facilidad para los comerciantes de llevar sus actividades a un entorno digital. Usualmente se usa la palabra extranjera *e-commerce* para referirse a las actividades y relaciones comerciales mencionadas que se desarrollan a través de los diferentes entornos digitales.

Para Feldstein & Scotti, comercio electrónico es:

> Una modalidad de comercio en la que la mediación entre la oferta y la demanda y el perfeccionamiento de las transacciones entre ellas se realiza a través de medios digitales de comunicación, ya sea por redes abiertas o cerradas, en un mercado virtual que no posee límites geográficos (fronteras) ni temporales y no tiene una ubicación determinada, porque se encuentra en el ciberespacio. (Citado por González & Albornoz, 2014, p. 8)

De acuerdo con esta definición, el comercio electrónico se desarrolla en un espacio digital mediante aplicaciones, páginas web u otro ciber lugar que media el uso de internet, por lo tanto, se identifica un nuevo ámbito de relaciones comerciales en el cual se debe garantizar la protección al consumidor, mediante la debida vigilancia y control a través de la Superintendencia de Industria y Comercio.

En relación con los tipos de comercio electrónico que se realizan en la actualidad, se encuentran:

- Comercio electrónico B2C: Es el desarrollado en el entorno digital, de negocio a consumidor individual.
- Comercio electrónico B2B: Las relaciones comerciales se realizan de un negocio a otro negocio.
- Comercio electrónico C2C: Desarrollado entre consumidor a consumidor.
- Comercio electrónico Social: se realiza a través de las redes sociales.
- Comercio electrónico móvil o m-commerce: Las transacciones y comercio realizado mediante el uso de dispositivos móviles.

  (Laudon & Guercio, 2013)

### 1.1.5. Red Social

Una red social es un sistema abierto de comunicación conformado por un conjunto de usuarios conectados que entablan conexiones con otros usuarios con gustos o intereses afines. La red social es un término propio del siglo XXI. La RAE define la red social como un servicio que

> ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes (Real Academia Española [RAE], 2020c, p. 1)

La red social supone una interconexión digital, *on line*, mediante el uso de internet puede ser a través de una aplicación o una página web que permite la comunicación, entre otros servicios, de una gran cantidad de usuarios. A principios de la década del 2000, la red social Facebook fue

la primera en ser reconocida a nivel mundial, desde esta época han surgido otras como *Twitter*, *Instagram, Tik Tok.*

Facebook, es una de las grandes compañías que presta servicios digitales a través de plataformas, *apps* y páginas web; entre otras se mencionan a Google, Amazon y Appel cada una con diferentes servicios. Desde hace menos de una década debido a la masificación del acceso a la internet, se potenció el uso de los productos ofrecidos por estas empresas, generando así el grupo GAFA, generando un nuevo marco económico al usar como moneda digital los datos personales de los usuarios que hacen uso de los servicios prestados, generalmente, mediante contratos de publicidad particularmente, y el uso de los diferentes programas de IA que fomenta la minería de datos.

En cuanto a los datos personales como moneda digital y la trascendencia que tiene esta en el mundo económico, se evidencia, por ejemplo, en el último reporte sobre los ingresos de Facebook publicado por la empresa Statista, la cual afirma "ascendieron a más de 70.500 millones de dólares estadounidenses, un valor récord que representa un incremento de más del 26% con respecto a 2018" (Fernández, 2020, p.1)

### 1.1.6. Inteligencia Artificial (IA)

La inteligencia Artificial, es un concepto propio de los avances tecnológicos en especial de lo que se conoce como la cuarta revolución industrial. Lo que antes no trascendía los límites de la ciencia ficción ahora encuentra camino en la IA, la cual, según Kaplan & Haenlein es "la capacidad de un sistema para interpretar correctamente datos externos, para aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible" (citado por Sanjuán Rodríguez, 2019, P. 82) y para mayor acierto, Rodríguez señala que la "IA es la tecnología que intenta asemejarse o superar las capacidades intelectuales del hombre" (2019, P. 83)

### 1.1.7. Minería de datos

Debido al gran flujo de datos personales mediante el uso de tecnologías y a la necesidad de realizar estudios y análisis sobre los mismos, surge la minería de datos como una respuesta permitiendo optimizar el análisis de los datos recolectados y almacenados en las bases de datos. Para Witten

& Frank la minería de datos es “el proceso de extraer conocimiento útil y comprensible, previamente desconocido, desde grandes cantidades de datos almacenados en distintos formatos”. (citado por Hernández, Ramírez & Ferri, 2004, p.) A su vez, Microsoft la define como “el proceso de detectar patrones significativos en los datos” (Microsoft, 2020, p.1) El objetivo principal de la minería de datos es ofrecer, predicciones y perfilamientos con base en los datos recolectados y analizados.

### 1.1.8. Plataforma de Comercio Electrónico

Una plataforma digital es un sistema creado para brindar servicios a través de aplicaciones o sitios web mediante el uso de la internet. Las plataformas digitales están diseñadas para prestar diferentes servicios de acuerdo a los objetivos de la empresa o sociedad que la crea. Una plataforma de comercio electrónico está dedicada a brindar un espacio apto para el desarrollo de relaciones comerciales mediante el uso de la internet, esta plataforma sirve como puede para ejecutar las aplicaciones o páginas web contenidas en ella.

Ahora bien, en cuanto a los portales de contacto o markectplace como Amazon, Ebay, Mercado libre, Olx, en los cuales además de mediar el uso de una plataforma electrónica o digital, realizan un alto TDP para realizar sus operaciones comerciales, la ley 1480 del 2011 o estatuto del consumidor, en el artículo 53, define los portales de contacto como

Quien ponga a disposición una plataforma electrónica en la que personas naturales o jurídicas puedan ofrecer productos para su comercialización y a su vez los consumidores puedan contactarlos por ese mismo mecanismo, deberá exigir a todos los oferentes información que permita su identificación, para lo cual deberán contar con un registro en el que conste, como mínimo, el nombre o razón social, documento de identificación, dirección física de notificaciones y teléfonos. (Ley 1480, 2011, art. 53)

### 1.1.9. Profiling

El perfilado de datos o profiling, es una práctica reciente que tomó auge con la masificación de los TDP en el entorno digital. Esta actividad facilita el análisis de los usuarios y/o consumidores en el entorno digital, permitiendo identificar sus gustos, intereses e incluso, sus decisiones, facilitando

la creación de grupos caracterizados o segregados para determinar a quienes se deben dirigir los anuncios y/o publicidades. Según Cambridge Dictionary, profiling es "la actividad de recolectar información acerca de alguien, especialmente un criminal, a partir de la descripción obtenida de ellos" (2020, p. 1), mientras que la RAE, define el perfilado como "la acción o efecto de perfilar" (2020b, p. 1) que a su vez se define como "dar o presentar el perfil de alguien o algo" (RAE, 2020a, p. 1)

## 1.2. Marco Normativo

### 1.2.1. Disposiciones que protegen el derecho a la intimidad y la privacidad.

En el marco internacional, la protección de habeas data tiene su fundamento en el derecho a la intimidad, desde organismos y disposiciones internacionales, hasta la Constitución Política colombiana, consagran el derecho a la intimidad y a la privacidad como un derecho humano, según el cual, a grandes rasgos, la persona no puede ser molestado en su vida privada o familiar, tampoco puede ser objeto de injerencias arbitrarias que afecte contra su derecho. En el plano internacional, se identifican las siguientes disposiciones en materia de protección a la intimidad y la privacidad:

- El artículo 5 de la Declaración Americana de los Derechos del Hombre y el Ciudadano consagra la protección de la honra, su vida privada y familiar frente a los ataques abusivos. (Asamblea General de las Naciones Unidas [ONU], 1789, art. 5)
- El artículo 12 de la Declaración Universal de Derechos Humanos establece el derecho a no ser objeto de injerencias en su vida privada, familiar e igualmente la protección a la honra y reputación del sujeto de derecho. (ONU, 1948, art. 12)
- El artículo 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos consagra los derechos respectivamente a la vida privada y familiar, y el derecho a la libertad de expresión. (ONU, 1966, art. 17-19)
- El artículo 11 de la Convención Americana sobre Derechos Humanos, establece el derecho a la honra y la dignidad consagrando la prohibición de injerencias arbitrarias que afecten la vida privada y la familia, y la obligación de los Estados de proteger a través de la ley este derecho. (Asamblea General de la Organización de Estados Americanos, 1969, art. 11)

Se diseña así un marco mínimo supranacional de protección a los derechos a la intimidad y la privacidad, que tiene como fundamento los derechos a la honra, la vida privada, la vida familiar del sujeto de derechos, se comprende la especial protección que debe tener el ámbito íntimo y privado de la persona; sin embargo, surge igualmente la protección al derecho a la libertad de expresión, esto no se traduce en un conflicto de derechos, sino en el reconocimiento de unas limitantes en cada uno de ellos.

### 1.2.2. Supranacional

#### *1.2.2.1. Resolución 45/95, Asamblea General de las Naciones Unidas.*

La Asamblea General de las Naciones Unidas (ONU), emitió la Resolución 45/95 el 14 de diciembre de 1990 que consagró los "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales" (ONU, Resolución 45/95 de 1990, p.1). En esta resolución se consagran siete principios, el principio de finalidad, principio de licitud y lealtad, principio de exactitud, principio de acceso de la persona interesada, principio de no discriminación, facultad de establecer excepciones y principio de seguridad; además señala que el control y vigilancia estará a cargo del ente creado por el Estado de acuerdo al ordenamiento interno (ONU, Resolución 45/95 de 1990, pp.1-2).

A su vez, establece que en el flujo de datos trasfronterizo debe contar con un nivel adecuado de protección de datos que ostenta cada Estado para establecer la limitación o no de esta práctica. Para Remolina, "la expresión adecuado se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador" (Remolina, 2010, p. 497), igualmente, Remolina señala que el principio de continuidad de protección de datos personales busca "garantizar que el nivel de protección sobre los datos personales de los ciudadanos de un país, no disminuya cuando los mismos deben ser exportados o transferidos a otro (s) país (es)" (Remolina, 2015, p. 37).

En lo que respecta al principio de finalidad, exactitud y facultad de establecer excepciones, permite al sujeto de derechos establecer límites sobre el TDP. En el caso del principio de finalidad, es preciso resaltar el apunte hecho por el autor citado Remolina, mediante los aportes realizados

por el grupo GECTI a la propuesta de la actual ley estatutaria 1581 de 2012 al señalar que, colombiana, el principio de finalidad implica la obligación de no realizar tratamientos de datos personales incompatibles a los autorizados previamente, además proponen que estos no deben ser excesivos remitiéndose a la proporcionalidad de los mismos (Remolina, 2011, p.5).

Los principios generales propuestos por la ONU establecen un mínimo de protección frente al TDP, busca asegurar el derecho a la privacidad de los sujetos de derechos a los que pertenecen los datos personales recolectados para ser tratados. A su vez, consagra un marco base de acción que deben hacer cumplir los Estados a través de las autoridades designadas.

#### *1.2.2.2. Directivas relativas a la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, OCDE.*

La reciente adhesión de Colombia a la Organización para la Cooperación y el Desarrollo Económico (OCDE), trajo una serie de requisitos mínimos que debía cumplir el país para ser miembro parte de esta organización. Durante el proceso de adhesión, Colombia tuvo que realizar un estudio acerca de la efectividad de sus políticas públicas además de evaluar los retos que implica estar dentro de los 37 países miembro de la organización. La OCDE, por su parte, es una organización que busca el desarrollo económico y la garantía de los derechos humanos mediante la promoción de políticas públicas que establecen estándares de bienestar los ciudadanos.

El 23 de septiembre de 1980, la OCDE dirigió cuatro recomendaciones a los Estados parte, acerca de la protección de la privacidad y el flujo trasfronterizo de datos personales. La OCDE, reconoce el deber de protección de la privacidad y la libertad de la persona o sujeto de datos, y a su vez expone la necesidad de permitir el flujo trasfronterizo de datos personales sin más limitantes que aquellas que aseguran la protección de los mismos. Así lo señala la organización al indicar que: “los Países Miembros deberían tomar todas las medidas oportunas y razonables para garantizar que los flujos transfronterizos de datos personales” (OCDE, 1980, p.6)

Estas directrices, a su vez, consagran ocho principios que se trazan como derrotero que han de seguir los Estados parte para alcanzar ese nivel adecuado, según la OCDE son:

Tabla 1. Principios propuestos por la OCDE.

| Principio | Descripción |
|---|---|
| Principio de limitación de recogida | Pretende asegurar la calidad de los datos que son recolectados |
| Principio de calidad de los datos | De acuerdo al fin por el cual fueron recolectado los datos, estos deben corresponder a información correcta y necesaria |
| Principio de especificación de los fines | Contempla la obligación de informar sobre alguna modificación frente a los fines iniciales establecidos previamente |
| Principio de limitación de uso | Los datos personales no deberían ser revelados ni usados bajo otros fines, a menos que cuente con el consentimiento previo por parte del titular de datos o bien, por un mandato legal |
| Principio de salvaguarda de la seguridad | A través de los medios de protección frente a perdidas, accesos no autorizados, revelación de datos entre otros |
| Principio de transparencia | Propone la creación e implementación de políticas públicas dirigidas a las empresas públicas o privadas que realicen TDP. Además, propone el establecimiento de los medios que verifiquen la finalidad y uso de los datos personales, la identidad y el domicilio del *inspector de datos* |
| Principio de participación individual | **Consagra la posibilidad del sujeto de datos de acceder a un canal de comunicación activa con quien está haciendo uso del tratamiento de sus datos personales, permitiéndole obtener información sobre el TDP** |
| Principio de responsabilidad, | Establece la responsabilidad del inspector de datos frente al TDP. |

*Nota. Principios contemplados por la OCDE para alcanzar un nivel adecuado de protección de datos personales. Adaptado de (OCDE 1980, pp. 5-6). Por Yahaira Arévalo Aragón, 2020

La OCDE, señaló igualmente las siguientes directrices sobre la implantación nacional en los Países parte:

> Los Países miembros deberían ocuparse en especial de:
>
> a) aprobar la legislación nacional adecuada;
>
> b) fomentar y respaldar la autorregulación, bien en forma de códigos de conducta o de otra manera;
>
> c) facilitar los oportunos medios para que las personas físicas puedan ejercer sus derechos;
>
> d) procurar las oportunas sanciones y soluciones en caso de incumplimiento a través de medidas que pongan en práctica los principios establecidos en las Partes Segunda y tercera;
>
> e) garantizar que no haya discriminación desleal contra los sujetos de los datos.
>
> (OCDE, 1980, pp.6-7)

Si bien, la Resolución emitida por la OCDE no ejerce efectos vinculantes si se presenta como un camino a seguir por los países que desean proteger el derecho a la privacidad y en sí, las libertades individuales. La Resolución está acompañada de un estudio de los temas que más afecta la protección a la privacidad en cuando al TDP, uno de los puntos clave son el empleo de Inteligencia Artificial y cualquier actividad automatizada de recolección y TDP. El enfoque de la Resolución es direccionar la protección en cabeza del Estado a través de políticas públicas y normativización que haga efectiva la protección de la privacidad y los datos personales de los sujetos de datos.

Además, posterior a las directrices de la OCDE de 1980, se emitieron las siguientes normas:

Tabla 2. Disposiciones emitidas por la OCDE desde 1980 en materia de Habeas Data.

| Disposición | Fecha | Descripción |
|---|---|---|
| Declaración ministerial sobre la protección de la privacidad de las redes globales | 7 y 9 octubre 1998 | Reafirma la protección de la privacidad de las redes globales y procuran a su vez, por la ausencia de limitación de flujo de datos trasfronterizos al asegurar un nivel de protección de datos personales. (OCDE, C (98)177, 1998) |
| Directrices para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas | [C (2003)116] 11 de junio 2003 | Promueve la implementación de políticas públicas en los Estados miembro, para la prevención de las actividades fraudulenta y engañosas que afectan a los consumidores durante la experiencia en el comercio electrónico, y en las actividades transfronterizas. (OCDE, C (03)116, 2003) |
| Declaración de Seúl sobre el Futuro de la Economía de Internet | [C (2008)99] 16 junio 2008 | Promueve la protección de la privacidad, la libertad de expresión y el acceso a internet; además señala la importancia de la gobernanza de internet como mecanismo para potenciar el uso de la tecnología digital y regular su futuro. (OCDE, C (2008)99, 2008) |
| Revisión Directivas Relativas a la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (1980) | Septiembre 2013 | La revisión realizada por la OCDE, deja intacto el núcleo básico de principios generales de protección de datos personales, y refuerza áreas como la responsabilidad demostrada o *accountability*. (OCDE, 2013) |
| Recomendación del Consejo sobre la protección al consumidor en el comercio electrónico | [C (2016)13] 24 marzo 2016 | Aplicable a las relaciones de comercio electrónico B2C, bajo la aplicación de los principios que rigen esta relación, regulando su actividad y proponiendo mecanismos de solución en caso de controversias. |

*Nota:* *Disposiciones recientes emitidas por la OCDE desde 1980 hasta la actualidad en materia de protección de datos personales, flujo transfronterizo de datos personales y comercio electrónico. Por Yahaira Arévalo Aragón, 2020

### 1.2.3. Principios y recomendaciones preliminares sobre la protección de datos, OEA.

La Asamblea de la Organización de Estados Americanos (OEA), siguió el ejemplo de la Unión Europea y el Consejo Europeo y diseñó una disposición aplicable al territorio americano que busca la protección de los datos personales. Mediante un estudio realizado por la OEA durante la primera década del siglo XXI, se logró determinar la importancia de los contextos jurídicos que estaban experimentando los Estados a partir del uso de nuevas tecnologías, de hecho, en un informe presentado ante la Asamblea General en el año 2007 se evidenció el impacto de campos como la medicina y la biotecnología sobre el TDP (OEA, CP/CAJP-2921/10, 2011).

Esta disposición está conformada por quince principios y recomendaciones que están diseñados para procurar por la protección de los datos personales, así, entre los más destacados se encuentra el principio del propósito específico, traducido en un propósito inequívoco sobre el uso de datos personales, este propósito debe ser conocido por el titular que autoriza su tratamiento; principio limitado y necesario, el TDP debe estar dirigido a un propósito proporcional, no excesivo, que busque una función específica; principio de transparencia, la posibilidad que tiene el titular de datos para establecer una relación con el recolector de datos o en general con su tratamiento. (OEA, CP/CAJP-2921/10, 2011)

Además, la OEA dedica un capítulo a la generación de "medidas proactivas y cooperativas" (OEA, 2011, p.14) dedicada a diseñar un marco de acción para los Estados parte, con el fin que cada Estado cree un marco adecuado de protección de datos a través de la educación y comunicación de las medidas implementadas para brindar espacios de protección al Habeas data.

A su vez, la Unión Europea ha emitido diferentes disposiciones que regulan la protección de datos personales en Europa, estas disposiciones son de especial importancia como referencia para el marco nacional, puesto que deseñaron un derrotero para la protección al habeas data, entre las disposiciones más destacadas por la materia que regulan, se encuentran

Tabla 3. Disposiciones en materia de protección de datos personales en Europa.

| Disposición | Fecha | Materia |
|---|---|---|
| Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal | 28 enero 1981 | -Respeto de los derechos y libertades de las personas.<br>-Protección al derecho a la vida privada.<br>-Principios básicos para la protección de datos personales. |

Tabla 3. Continuación

| | | |
|---|---|---|
| Directiva 95/46/CE<br>Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. | 24 octubre 1995<br>(en vigor hasta mayo 2018) | -Principio generales de protección de datos personales.<br>-Protección al derecho a la intimidad con respecto al tratamiento de datos personales. |
| Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas | 12 julio 2002 | -Garantiza los derechos y libertades de las personas físicas en cuanto a tratamiento de datos personales.<br>-Confidencialidad de comunicación.<br>-Limitación al uso de datos de tráfico cuando ya no son necesarios. |
| Carta de Derechos Fundamentales de la Unión Europea | 7 diciembre 2002 | -Artículo 7, espeto de la vida privada y familiar<br>- Artículo 8, derecho a la protección de los datos personales.<br>-Artículo 51, deber de las instituciones y los organismos de la UE de garantizar y respetar este derecho. |
| Reglamento (UE) 2016/679<br>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, derogó la Directiva 95/46 CE. | 27 abril 2016 | -Protección al derecho a la protección de los datos personales.<br>-Prohíbe la limitación a la libre circulación de los datos personales en la Unión, por protección de datos.<br>-Tratamiento de categorías especiales de datos personales. (datos sensibles) |

*Nota*: *Estas disposiciones fueron emitidas por los organismos europeos y se encuentran relacionadas en el Manual de Legislación Europea en materia de protección de datos, publicado por la Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, (2019). Por Yahaira Arévalo Aragón, 2020

### 1.2.4. Red Iberoamericana de Protección de Datos (RIPD)

La Red Iberoamericana de Protección de Datos (RIPD), surgió en el año 2003 en Guatemala mediante el acuerdo logrado durante el Encuentro Iberoamericano de Protección de Datos (EIPD). La RIPD se configuró como un foro que busca fomentar la protección de datos personales en los países iberoamericanos mediante la concertación de principios, mecanismos y normativas en materia de protección de datos. A su vez se encuentra mediada por una amplia cooperación entre los Estados que forman parte de esta red, generando así un marco generalizado, iberoamericano, de protección de datos personales (RIPD, 2019).

La conformación de la RIPD se encuentra fortalecida a partir de las autoridades y agentes que crea cada Estado para fomentar y garantizar la protección de datos a nivel nacional, los cuales se encuentran establecidos en el reglamento aprobado durante el VI Encuentro Iberoamericano de Protección de Datos y mediante la Declaración del XVII EIPD sobre el estado de las Autoridades Iberoamericanas de Protección de Datos (RIPD, 2019). A la fecha, la RIPD ha realizado diecisiete encuentros desde su fundación, en cada uno se han debatido temas sobre la protección de datos personales, la implementación de la inteligencia artificial (IA), los principios generales, el comercio electrónico entre otros.

Del mismo modo, en junio del año 2017, la RIPD emitió los Estándares de protección de datos personales para los estados iberoamericano, en el cual se consagro como objetivos principales el establecimiento de un conjunto de principios y derechos de protección de datos personales, elevar la protección de los datos personales durante su tratamiento, garantizar el ejercicio y tutela del derecho de habeas data, facilitar el flujo de datos personales entre los Estados Iberoamericanos e implementar los mecanismos para la cooperación internacional (RIPD, 2017, p. 12)

Los principios establecidos por la RIPD son:

- Principio de legitimación.
- Principio de licitud.
- Principio de lealtad.
- Principio de transparencia.
- Principio de finalidad.
- Principio de proporcionalidad.
- Principio de calidad.
- Principio de responsabilidad.
- Principio de seguridad.
- Principio de confidencialidad.

(RIPD, 2017, p. 2)

De igual forma, se determinó los ámbitos de aplicación subjetivo, objetivo y territorial, llamando especial atención el último ámbito al señala que estos estándares se aplicaran cuando el

TDP sea realizado "por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales" (RIPD, 2017, p. 15) Además, incluyó la facultad para ponderar el derecho de protección de datos personales con otros derechos fundamentales y libertades, es decir, que estos Estándares consideran la protección de datos como un derecho fundamental. Del mismo modo, señala los principios generales aplicables para el TDP, entre los cuales incluye el principio de proporcionalidad según el cual "el responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento" (RIPD, 2017, p. 20) e incluso consagro el derecho a obtener asistencia no automatizada y exigir la asistencia humana durante el ejercicio de las decisiones emanadas de los contratos que celebre el usuario o consumidor y el responsable o encargado del TDP; para lo cual contempla la posibilidad de impugnar la decisión individual automatizada (RIPD, 2017, p. 25)

Los Estándares de la Red, son una disposición prometedora en materia de protección de datos personales, al señalar entre sus postulados condiciones y exigencias que permiten asegurar un nivel adecuado de protección de datos personales, incluso en la misma medida que lo hace la Unión Europea y el Consejo Europeo.

## 1.3. Nacional

### 1.3.1. Constitución política de 1991.

El camino constitucional que ha recorrido el derecho al Habeas Data a partir de la Constitución Política de 1991 (C.P.C), inicia bajo la interpretación de los derechos consagrados en el artículo 15 constitucional esto es, el derecho a la intimidad, el derecho al buen nombre y el derecho al habeas data (C.P.C., 1991). Lo primero que hay que decir, es que el derecho al habeas data se presenta como un derecho fundamental autónomo, y que en ningún caso equivale al derecho a la intimidad, pero si se fundamenta en este. El artículo 15 señala por un lado la obligación constitucional del Estado colombiano de respetar y hacer respetar estos derechos y por otro el "derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas" (C.P.C., 1991, art. 15). Sin embargo,

estos no son los únicos derechos que reconoce el habeas data, según la Corte Constitucional, se debe incluir a las facultades consagradas en el artículo 15 ibidem, aunque no corresponde a una lista taxativa, el poder "autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos" (Corte Constitucional, Sentencia C-748, 2011), e incluso "la limitación en la posibilidad de divulgación, publicación o cesión" (Corte Constitucional, Sentencia T-729, 2002).

De manera análoga, el segundo párrafo del artículo 15 señala "en la recolección tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en Constitución" (Const., 1991, art. 15) es necesario remitirse al artículo 16 ibídem que consagra el derecho fundamental a la libertad de expresión, el artículo 28 como cláusula general del derecho a libertad; y la protección constitucional desde el tipo de Estado fundado en principios rectores de libertad y dignidad humana lo que nutre este postulado de mayor trascendencia.

Ahora bien, este derecho, como se mencionó es fundamental y autónomo, incluye la facultad del sujeto de derecho de ejercer un control permanente sobre los datos personales usados por el recolector de datos, a partir de la extracción de la normativa en materia como lo es la Ley 1581 de 212, debe responder preguntas como: cuáles datos son usados (principio de calidad de recolección), por qué son usados (principio de finalidad), cómo son usados (principio de transparencia) y dónde son usados (principio de circulación restringida). Respecto a la facultad de actualización, implica la posibilidad que los datos personales tratados puedan ser reestablecidos cuando el dueño de los mismos, es decir la persona sobre la que recae los datos lo considere; por su parte, la rectificación permite al sujeto de derechos ejercer medios de corrección cuando considere que se presenta alguna inconsistencia frente al tratamiento de sus datos personales; esto es lo que la jurisprudencia nacional ha denominado autodeterminación informática fundada en el respeto a las libertades y protección de habeas data.

Del mismo modo, la Constitución consagra el derecho a la información en el artículo 20 que faculta a recibir información y dar a conocer información bajo la debida responsabilidad social, y el derecho de la rectificación bajo las condiciones de equidad (C.P.C., 1991). Si bien, el derecho a la información consagra como limitante la responsabilidad social, desde la protección de habeas data es pertinente apuntar que no toda información es libre de comunicarse. El derecho consagrado

en el artículo 20 ibidem para la Corte Constitucional tiene una dimensión activa que faculta el derecho a obtener información y otra pasiva, esto es, el derecho a recibirla, que en cualquiera de los dos casos puede recaer sobre datos personales, Sentencia C-748 (2011). Además, el mismo artículo, establece la facultad del sujeto de derechos de rectificar la información, lo que permite en un ámbito digital que el titular de datos pueda dirigirse a la entidad pública o privada, que, si bien gozan del derecho a la información, deben asegurar el ejercicio de los principios que rigen la reglamentación de la protección de datos personales. La rectificación de la información, y en especial, de los datos que son divulgados o tratados por recolectores de datos debe contar no solo con la posibilidad de corregir o rectificar los datos, sino eliminar y actualizar los mismos.

### 1.3.2. Ley estatutaria 1266 de 2008.

La Ley estatutaria 1266 fue declarada exequible mediante sentencia C-1011 del 16 de octubre de 2008 (Corte Constitucional, Sentencia C-1011, 2008). La Corte Constitucional realizó un estudio minucioso sobre las disposiciones de la ley 1266, desde la restricción del ámbito de aplicación de la norma hasta el régimen sancionatorio de la misma, por lo que es pertinente analizar dicha norma bajo algunas precisiones jurisprudenciales.

La Ley 1266 tiene por objeto la coyuntura de los derechos constitucionales consagrados en los artículos 15 y 20 de la Constitución, frente al tratamiento de información en las bases de datos personales financieras, comerciales, las que presten servicios y las originadas en terceros países (Ley 1266, 2008).

Su enfoque principal es el desarrollo y reconocimiento legal de la facultad que tienen los ciudadanos colombianos a conocer, rectificar y actualizar la información suministrada a las bases de datos de las empresas públicas y privadas que pertenecen al sector financiero y almacenan o realizan TDP de contenido crediticio que según el artículo 3 corresponde a los datos sobre el "nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les de origen" (Ley 1266, 2008, art. 3). De igual forma la Corte Constitucional al realizar el estudio del proyecto de ley, encontró que este ostenta una regulación parcial del derecho al habeas data y que no por ello constituye una omisión legislativa relativa en tanto no existe limitación constitucional que ordene crear leyes estatutarias genéricas, además

porque el derecho al habeas data sigue regulado por el artículo 15 constitucional (Corte Constitucional, Sentencia C-1011, 2008).

Lo primero a mencionar, son las excepciones a la ley 1266, entre estas se encuentra aquella que es recogida para garantizar la seguridad nacional por Inteligencia del Estado, los registros de las cámaras de comercio puesto que se rigen por disposiciones especializadas y "aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales" (Ley 1266, 2008, art. 2). Para la Corte, es acertada esta exclusión hecha por el legislador en tanto la recolección de datos que tiene por objetivo la seguridad nacional mediante actividades de inteligencia del Estado difiere de la recolección de datos que tiene finalidades financieras o comerciales, caso similar ocurre para las cámaras de comercio y el ámbito doméstico. (Corte Constitucional, Sentencia C-1011, 2008)

A su vez establece la distinción entre fuente de información y operador de información. La primera figura corresponde a quien recibe y por tanto conoce de los datos suministrados, la Ley señala que esta fuente de información puede ser una persona natural o jurídica, entidad u organización que recolecta información en virtud de una relación comercial, financiera, de servicio u otra. Por otro lado, el operador de información es quien "recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley" (Ley 11266, 2008, art. 3). Es decir que sobre el operador de información recae la responsabilidad de garantizar la protección de los datos recolectados y tratados según las disposiciones legales. La Ley también indica que un mismo sujeto puede ostentar la calidad de fuente de información y operador de información, en este caso adquiere las funciones y deberes simultáneos de cada una de las figuras (Ley 1266, 2008).

En cuanto a los principios consagrados en esta ley, el artículo 4 sobre los principios de la administración de datos establece los siguientes:

Tabla 4. Principios, Ley 1266 de 2008.

| Principio | Descripción |
|---|---|
| Principio de veracidad o calidad de los registros o los datos. | La información debe ser exacta, veraz, completa, actualizada, comprobable y comprensible. |
| Principio de finalidad | De acuerdo a la constitución y la ley previa información al titular de los datos. |
| Principio de circulación restringida | Señala la prohibición de compartir los datos personales por servicios de internet o cualquier otro medio de divulgación masiva a menos que se pueda controlar para brindar una información restringida a los autorizados por la ley. |
| Principio de temporalidad de la información | Según la finalidad establecida y autorizada por el titular de los datos. |
| Principio de integral de derechos constitucionales | Enfatiza en la protección de los derechos constitucionales principalmente del artículo 15 constitucional. |
| Principio de seguridad | Se debe consagrar las medidas necesarias para evitar filtración de información, perdida, adulteración o cualquier actividad que afecte la protección de los datos. |
| Principio confidencialidad. | Establece la obligación de las personas naturales o jurídicas de naturaleza no pública de garantizar la reserva de información incluso con posterioridad a la relación que generó el TDP. |

*Nota*: *Relación de Principios sobre protección de datos personales según la ley 12266 de 2018. Por Yahaira Arévalo Aragón, 2020

Sin embargo, estos principios son de aplicación sectorizada, al igual que cada una de las disposiciones de la ley 1266, por versar únicamente sobre el habeas data financiero. Además, respecto a la posibilidad de entregar información recolectada para favorecer la circulación de la misma, la ley consagra en su artículo 5, los ámbitos en que se deben dar, se presta particular atención el literal c, que señala:

> A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos (Ley 1266, 2008, art. 5).

En este apartado, se identifica la posibilidad de compartir, o bien, circular datos personales contenidos en una base de datos inicial por un operador a quien fue reconocido la facultad de TDP

por el titular de los datos, y pasar luego a un operador diferente al autorizado por el titular de los datos. Si bien este literal consagra la obligación que la circulación de datos tenga como limitación el principio de la finalidad, esto puede resultar en una afectación a los derechos del titular de datos por cuando al cambiar el operador se debería especificar esta posibilidad, de lo contrario, la autorización inicial en principio no tendría el mismo sentido por ser un operador diferente; sin embargo, al estar consagrado en la ley, y previo aviso al titular este se convalidaría.

Sobre los derechos que tienen los titulares de datos al momento de autorizar el TDP, se incluyen todos aquellos correspondientes al Habeas data, los del artículo 15 y el artículo 20 constitucional. El parágrafo del artículo 6 señala que los datos privados y semiprivados siempre requerirán del consentimiento previo y expreso del titular para el TDP, aunque se excepcionan los datos financieros, crediticios, comercial, de servicios o aquel que trata de flujo de datos transfronterizos siempre que no se desmejore la protección de los datos y teniendo en cuenta los principios de la administración de datos. (Ley 1266, 2008) En cuanto a esto, la Corte precisó que respecto a los datos sensibles y la posibilidad de TDP desde el sector regulado por la ley 1266 queda proscrito. (Corte Constitucional, Sentencia C-1011, 2008) De igual forma señaló que no existe presunción de datos públicos al estudiar el concepto de datos públicos en el entendido que el legislador define los conceptos dato semiprivado y dato privado. (Corte Constitucional, Sentencia C-1011, 2008)

La Superintendencia de Industria y Comercio (SIC), realizó una cartilla sobre la Ley 1266, en la cual señaló los pasos que se llevan a cabo bajo la ley, para la recolección y el TDP en el sector financiero, estos son: una autorización expresa y previa con fines delimitados, la posterior recolección por la fuente de información de los datos, el envío de los datos recolectados al operador de información, reportando el cumplimiento de un pago o un estado moratorio, el operador recibe los datos, el usuario de la información puede consultar la información recolectada por el operador. (SIC, 2020)

La ley 1266, tiene un ámbito específico de aplicación al limitarse a la regulación del Habeas data financiero. Si bien es una ley estatuaria pues se fundamenta en los artículos 15 y 20 Constitucional, la Corte Constitucional estableció su carácter especializado, señalando:

> Para el caso del Proyecto de Ley, su temática está relacionada con la determinación de las reglas destinadas a regular el ejercicio del derecho a la autodeterminación informática o hábeas data de los titulares de información contenida en bases de datos personales, en especial aquellos datos de contenido financiero, crediticio, comercial, de servicios y la proveniente de terceros países (Corte Constitucional, sentencia C-1011, 2008).

Cabe mencionar que esta caracterización se ve aún más delimitada al identificarse el objeto principal de la ley 1266, es la recolección de datos de los usuarios de sectores financiero, crediticio, comercial y de servicios, para realizar cálculos de riesgo crediticio. Por ello, la misma ley contempla tipos de datos particulares que corresponde a los datos positivos o negativos, pero ellos no versan sobre la totalidad del campo del Habeas data, ni regula su administración en otros ámbitos.

### 1.3.3. Ley estatutaria 1581 de 2012.

La ley sobre las disposiciones generales para la Protección de Datos Personales es el resultado de lo propuesto por la Corte Constitucional en la sentencia C-1011, cuando señaló la importancia de regular el marco general de Habeas data, es decir, aquel campo que no reguló la ley 1266.

Lo primero a mencionar de la ley 1581, fue declarada exequible por la Sentencia C-748 del 2011. El objeto de la 1581, en principio busca, igual que la ley 1266 desarrollar los derechos contenidos artículo 15 y 20 constitucionales, sobre todo los que refiere a la facultad del titular de datos, no solo a conocer, actualizar y rectificar cualquier información suministradas a las bases de datos de entidades públicas o privadas, sino también la capacidad de “autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos de una base de datos o archivo” (Corte Constitucional, Sentencia C-1011, 2008). Es decir que, la ley 1581 surge como marco general de protección al derecho del habeas data, integrado por el derecho a la autodeterminación informativa y el derecho al libre desarrollo de la personalidad, al no tener contenido de disposiciones sectorizadas, fomentando un modelo hibrido de protección de habeas data. Además, la ley 1581, bajo una interpretación exegética de la norma y a partir de la respuesta del 17 de julio de 2020 emitida por la DIPDP, explicó que la norma extiende el campo de aplicación territorial al señalar que es aplicable a cualquier empresa, pública o privada, incluso extranjera, que realice TDP de ciudadanos colombianos, dentro del territorio, siempre que se sigan las disposiciones

internacionales vigentes. (Dirección De Investigación De Protección De Datos Personales (DIPDP), 2020).

En cuanto a las excepciones de la ley 1581, menciona la información del ámbito doméstico, aquella de inteligencia y contrainteligencia, defensa nacional, la recolectada bajo la ley 1266 de 2008 y la ley 79 de 1993 (Ley 1581, 2012).

La ley 1581, consagró principios generales para el TDP, que deben ser considerados en todos los ámbitos y sectores, incluso si se presenta una disposición especial estos deberán ser considerados de manera concomitante, así lo señala el artículo 2 de la misma. A su vez, la Corte, estableció que la inclusión del párrafo del artículo 2 obedece al carácter general de aplicación de la norma y a la debida aplicabilidad que debe tener los principios para la resolución de casos particulares sobre PDP. (Corte Constitucional, Sentencia C-748, 2011)

Los principios rectores que establece la ley 1581 son:

| | |
|---|---|
| Principios habeas data, Ley 1581 de 2015. | Principio de legalidad. El TDP es una actividad reglada. |
| | Principio de finalidad. |
| | Principio de libertado. Obligación de obtener siempre la autorización y el consentimiento expreso, previo e informado |
| | Principio de veracidad o calidad de los datos. |
| | Principio de transparencia. Garantiza al titular de los datos, realizar cualquier solicitud dirigida al responsable o encargado del tratamiento, para obtener información en cualquier momento y sin restricciones |
| | Principio de acceso y circulación restringida. |
| | Principio de seguridad. |
| | Principio de confidencialidad. |

Figura 1. Principio de PDP, ley 1581 de 2012. Por Yahaira Arévalo Aragón, 2020

Además, la ley 1581, establece la prohibición, dentro del principio de acceso y circulación restringida, que los datos personales, excluyendo los tenidos por información pública “no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el

acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley" (Ley 1581, 2012, art. 4). Esta disposición presenta la primera limitación a la circulación sin restricciones de los datos personales de los usuarios de internet a través de plataformas de comercio electrónico, redes sociales y demás entornos digitales, donde el TDP se ha vuelto una práctica necesaria para la prestación de los servicios de las empresas. A su vez, la ley 1581, señala la prohibición de la transferencia de datos personales a terceros países, que no cuenten con el nivel adecuado de protección de datos personales para su tratamiento (Ley 1581, 2012).

Ahora bien, en lo que respecta a los datos sensibles, partiendo de la definición según la cual son aquellos que afectan a la persona por la posibilidad de presentarse situaciones de discriminación al afectar su intimidad; la ley 1581 refuerza la obligación de respetar los datos sensibles de los titulares de datos e incluso establece la regla general prohibitiva de tratamientos de datos, y por el contrario señala las excepciones a la regla en las cuales se puede llevar a cabo esta actividad, siempre y cuando medie autorización expresa y previa del titular de los datos. La solicitud de información por parte del titular de datos, dirigida al responsable o encargado del tratamiento, es un derecho, y le permite dar efectividad al artículo 15 constitucional, al facultarlo para conocer el uso ejercido sobre sus datos personales; en caso de encontrar alguna vulneración a los principios y derechos que le asisten, puede revocar la autorización mediante queja dirigida ante la SIC, para que esta ordene si es el caso el termino de dicha autorización. Así, la autorización del titular se convierte en un requisito legal y constitucional para la actividad de TDP.

Aquí es preciso diferenciar las figuras de responsable de TDP y encargado de TDP. El primero, según la ley en mención, se refiere a aquel que "decida sobre la base de datos y/o el Tratamiento de los datos" (Ley 1581, 2012, art. 2). Mientras que el encargado de TDP es quien "realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento" (Ley 1581, 2012, art. 2). Al responsable y encargado del TDP le asisten entre otros, los siguientes deberes:

Tabla 5. Deberes del responsable y el encargado de TDP, Ley 1581, 2012.

| Responsable de TDP, artículo 17: | Encargado de TDP, artículo 18: |
|---|---|
| a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;<br>b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;<br>c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;<br>d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;<br>e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley; […]<br>g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;<br>h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad […]<br>j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella; | a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;<br>b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;<br>c)Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;<br>d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;<br>e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible; […]<br>j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley; […]<br>m) Informar a solicitud del Titular sobre el uso dado a sus datos;<br>n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.<br>o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio |

NOTA: Descripción del Art. 17 y 18 de la ley 1581, de 2012, Por Yahaira Arévalo Aragón, 2020

Igualmente, la ley consagra las autoridades de vigilancia y control que ejercerán funciones sobre el TDP, esta es la Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales, los trámites se indician a través de la SIC, bajo las disposiciones especializadas. En caso de vacíos legales se debe remitir al Código Contencioso Administrativo. Respecto a las sanciones, se prevén las multas, suspensión de actividades sobre TDP, cierre temporal, cierre inmediato o definitivo (Ley 1581, 2012). Por último, la ley 1581 de 2012 crea el Registro Nacional de Bases de Datos, reglamentado por el Decreto 886 de 2014, que funciona como “el directorio público de las bases de datos sujetas a Tratamiento que operan en el país” (Ley 1581, 2012, art. 25).

### 1.3.4. Decreto 1377 de 2013.

El Decreto 1377, reglamentó la Ley Estatutaria 1581, especialmente sobre los aspectos de la autorización del titular de datos, el TDP, las políticas y la responsabilidad demostrada en el TDP (Decreto 1377, 2013). Además, el Decreto 1377, agregó nuevas definiciones a la Ley 1581, entre las que destaca el aviso de privacidad, la transferencia y la transmisión.

En primer lugar, se debe señalar que la autorización para la recolección y TDP es el fundamento que legítima esta actividad y el resultado de la interpretación armónica de los principios a la finalidad y la libertad. El TDP está prohibido a menos que se cuente con la autorización explícita y previa, que según el artículo 5 del Decreto en mención debe ser "a más tardar en el momento de la recolección de sus datos" (Decreto 1377, 2013, art. 5). En dicha autorización se debe informar al titular de datos, cuáles datos personales serán tratados y cuál es la finalidad de cada uno de ellos, además según el numeral primero del artículo 6, se debe indicar al titular de datos que no está obligado a proporcionar la autorización para el tratamiento de sus datos sensibles (Decreto 1377, 2013). Respecto a las formas de obtener la autorización, se encuentran la usuales, escrita, oral, y se suma las conductas inequívocas del titular que permite concluir la autorización, sin embargo, el mismo señala que no es procedente el silencio como forma de autorización. Además, las autorizaciones tienen límites temporales según la necesidad y finalidad para la cual se recolectaron los datos.

Sobre las políticas de tratamiento, se convierte en un requisito obligatorio para los sujetos que desean realizar actividades de TDP. Deben informar al titular de datos sobre la razón social, domicilio, los derechos que le asisten, los tratamientos de datos a los que se verán sometidos, y en caso de la imposibilidad de presentar la política de tratamiento al titular de datos, se debe incluir el aviso de privacidad, sobre la existencia de la política de tratamiento y cómo acceder a ella (Decreto 1377, 2013).

En cuanto a la trasferencia y la transmisión internacional de datos, estos se deben realizar bajo un nivel adecuado de protección de datos personales, se debe observar las leyes en materia, y se permite cualquiera de las dos figuras sin la previa información al titular, cuando esta se realice en vigencia de un Contrato de Transmisión de datos personales. En este contrato, el encargado del

TDP, deberá adoptar las mismas obligaciones contraídas con el titular de datos, realizar actividades de TDP únicamente por lo autorizado por el titular de datos y manteniendo la política de tratamiento presentada al titular de datos. En cuanto a la diferencia entre la transferencia y la transmisión de datos, la primera figura tiene lugar cuando el responsable o encargado del TDP envía la información a un receptor fuera del país que tiene la misma calidad; mientras que, la transmisión es el tratamiento dentro o fuera del país, que se realiza "entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable" (Decreto 1377, 2013, art. 24).

Por último, el Decreto 1377 contempla la responsabilidad demostrada en la actividad del TDP, según la cual

> Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto (Decreto 1377, 2013, art. 26).

### 1.3.5. Decreto 886 de 2014.

El Decreto 886 de 2014, surge como resultado de la creación del Registro Nacional de Base de Datos y tiene por objetivo la reglamentación de este Registro. Se fundamenta en la Ley 1262016 de 2008 y la Ley 1581 de 2013 sobre protección de datos. Busca el registro de cada una de las bases de datos que realicen y contengan tratamiento manual o automatizado, dentro del territorio nacional o fuera de él. El registro nacional, permite dar cumplimento al derecho que le asiste al titular de datos de conocer las actividades, bases de datos, sujetos que realizan TDP y en general cualquier información que requiera para ejercer su derecho constitucional contenido en el artículo 15.

En consecuencia, el artículo 8 del decreto en mención señala que los canales de comunicación a disposición de los titulares de datos son la recepción y atención de peticiones, consultas y reclamos, a través de los cuales, el usuario puede ejercer su derecho a "conocer, actualizar, rectificar y suprimir sus datos personales contenidos en bases de datos y revocar la autorización que haya otorgado para el Tratamiento de los mismos, cuando esto sea posible" (Decreto 886, 2014, art. 8). Además, el mismo decreto señala las formas de TDP, resumiéndola en

tratamiento de datos automatizado y tratamiento de datos manual (Decreto 886, 2014). Definiendo cada una de las figuras mencionadas así, "son bases de datos manuales los archivos cuya información se encuentra organizada y almacenada de manera física y bases de datos automatizadas aquellas que se almacenan y administran con la ayuda de herramientas informáticas" (Decreto 886, 2014, art. 10).

Cabe mencionar que el decreto 886, tiene un campo de aplicación más dirigido hacia el sector financiero del que trata la ley 1266 de 2008 y que se fomenta con la Resolución 76434 del 2012 emitida por la Superintendencia de Industria y Comercio, en la cual se señalan cómo debe cumplirse las disposiciones de la ley 1266 en las actividades de TDP llevadas a cabo por el sector financiero, comercial, de servicios y de terceros países, vigilados por la SIC (SIC, Resolución 76434 de 2012).

### 1.3.6. Decreto Único Reglamentario 1074 de 2015.

El Decreto Único Reglamentario del Sector Comercio, Industria y Turismo expedido en el año 2015, compiló entre otras disposiciones, las establecidas en materia de protección de datos tanto del sector financiero como aquellas que regulan el habeas data de aplicación general, y las reunió en los siguientes capítulos:

- Capítulo 25 y capítulo 26, reglamentó la ley 1581 de 2012 y sus decretos reglamentarios Decreto 1377 de 2013 y Decreto 886 de 2014.
- Capítulo 27 y Capítulo 28, reglamentó la ley 1266 de 2008 y sus decretos reglamentarios Decreto 1727 de 2009 y Decreto 2952 de 2010.

  (Dirección de Investigación de Protección de Datos Personales, 2020)

Debido a que el Decreto en mención compiló en su totalidad las disposiciones en materia de habeas data es preciso indicar que según el artículo 3.1.1 del mismo señala la derogatoria integral de las disposiciones compiladas por el decreto, sin embargo, aún se siguen remitiendo a las normativas nacionales, con las notas de vigencia pertinentes.

### 1.3.7. Pronunciamientos jurisprudenciales y doctrina.

El habeas data o autodeterminación informática, en la jurisprudencia constitucional inició a partir del reconocimiento del *poder informático* como nuevo contexto digital que afectó la última década del siglo XX con el surgimiento de la internet. Desde sentencias como la T-414 del año

1992 o la T-307 de 1999 se evidencio una nueva realidad social, en la que los datos personales de quienes accedían a internet eran usados para realizar diferentes actividades de TDP y a su vez, almacenados en bases de datos y archivos para su uso (Corte Constitucional, Sentencia T-729, 2002).

Esta realidad social, provocó que el derecho al habeas data tuviera un desarrollo jurisprudencial amplio. Desde el reconocimiento del derecho al habeas data como un derecho fundamental autónomo, distinto al derecho a la intimidad y al buen nombre (Corte Constitucional, Sentencia T-552, 1997). A su vez, con las sentencias T-414 de 1992 señaló como respuesta al contexto tecnológico el surgimiento de una cuarta generación de derechos que dieran respuesta a los avances científicos y tecnológicos (Corte Constitucional, Sentencia T-414, 1992); y la sentencia T-022 de 1999 citadas en la sentencia T-729 de 2002, en la cual, la Corte identificó como características del dato personal

> i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida […] iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (Corte Constitucional, Sentencia T-729, 2002).

Las jurisprudencias citadas anteriormente fueron el inicio de una línea jurisprudencial sólida en materia de desarrollo de habeas data, incluso en su reconocimiento en el entorno digital, especialmente en lo que refiere a la recolección y TDP. Ahora bien, entre la primera y segunda década del siglo XXI, la Corte ha encontrado una nueva problemática referente al entorno digital, el uso de las redes sociales, aplicaciones y plataformas de comercio electrónico ha generado nuevos desafíos para la jurisprudencia colombiana.

Por ejemplo, en la sentencia T-260 de 2012, la Corte señaló que los derechos de los usuarios de las redes sociales como Facebook pueden verse afectados al momento en que comparten contenido digital o bien cuando sus datos son tratados por la compañía, de cualquier forma, esta vulneración puede ocurrir en el momento del registro, cuando participa en la misma o incluso cuando decide abandonarla (Corte Constitucional, Sentencia T-260, 2012). De igual manera, la

sentencia T- 634 de 2013, planteó de nuevo el debate sobre los riesgos del uso de las redes sociales y entornos digitales para la protección al habeas data señalando que

> La afectación de los derechos fundamentales en redes sociales como Facebook puede ocurrir no sólo respecto de la información que los usuarios de esta red social ingresan a la misma o cuyo ingreso permiten a través de su perfil, sino también con relación a información de personas, usuarias o no, que ha sido publicada y usada por terceros en las redes sociales. (Corte Constitucional, Sentencia T-634, 2013)

De igual manera, la Superintendencia de Industria y comercio, a través, de la Delegatura para la Protección de Datos Personales, ha emitido varias decisiones que buscan la protección del habeas data de los usuarios a quienes se les realiza TDP, entre las más recientes se encuentra:

Tabla 6. Resoluciones emitidas por la SIC en el año 2020 sobre protección de habeas data.

| Número de Resolución | Caso | Resuelve |
|---|---|---|
| Resolución 24913 DE 2020 | Resolvió recurso de apelación propuesto por el Banco de Bogotá. al considerar que no le era aplicable las disposiciones de la ley 1581/12, puesto que su sector es el regulado por la ley 1266/08, y por tanto no le era exigible registrar la base de datos en los términos de la ley 1581/12 | SIC encontró desestimada esta pretensión, debido a que "el ámbito de aplicación de la ley 1266 de 2008 se determina por el tipo de datos personales que se trata y los fines para que se utilizan, y no por la naturaleza del sujeto que usa esa información" (Resolución 24913, SIC, 2020) |
| Resolución 30412 de 2020 | Un fotógrafo fue contratado para realizar una sesión de fotos a la denunciante en un hotel, y posterior a ello, estas se publicaron en la Revista Caras, debido a una autorización de propiedad intelectual que firmó el fotógrafo. | Negar el recurso de apelación. La SIC, encontró que la autorización inicial de la denunciante no es suficiente para que el fotógrafo se otorgue la facultad de firmar dicha autorización, además al tratarse de datos sensibles por ser datos biométricos como las facciones, no pueden ser divulgados sin la observancia de la ley 1581/12. (Resolución 30412, SIC, 2020) |

Tabla 6. Continuación

| | | |
|---|---|---|
| Resolución 12192 de 2020 | Facebook se negó a acatar las órdenes dictadas por la SIC, al considerar que la SIC no tiene competencia jurisdiccional sobre la sociedad, además indicó que las medidas actuales de protección de datos eran suficientes. | Confirmó la resolución 1321 de 2019, mediante la cual ordenó a la sociedad Facebook, adecuaciones a su política de protección de datos, para fortalecer el cumplimiento de la ley 1581/12. La SIC, señala que tiene competencia de acuerdo a la normatividad colombiana y debido al TDP de usuarios colombianos realizado por medio de cookies, era pertinente conocer del caso. Además, señaló que en atención al principio *accountability*, la Sociedad Facebook debía ser capaz de demostrar la eficiencia de sus políticas de protección de datos. (Resolución 12192, SIC, 2020) |

Nota *: Resoluciones emitidas por la SIC durante el año 2020, en materia de protección de datos personales. SIC (2020). Normatividad. Resoluciones sobre Protección de Datos Personales. Por Yahaira Arévalo Aragón, 2020

De igual forma la SIC a través de la DIPDP, señaló qué de manera complementaria se han elaborado guías que detallan las disposiciones descritas en la ley 1581, las cuales desarrollan, como método complementario, la protección de datos personales en Colombia. (DIPDP, 2020).

## 2. Modelo europeo y estadounidense de protección de habeas data.

Lo primero a mencionar, es que en la actualidad se reconocen dos modelos de protección de datos personales, estos son el modelo europeo y el modelo estadounidense. El modelo europeo está conformado por disposiciones como el Reglamento General de Protección de Datos y el Convenio 108 sobre el Tratamiento de Datos Automatizado de Carácter Personal, este modelo se caracteriza por una amplia protección del Estado frente a los tratamientos de datos personales, además que desde el RGPD el derecho a la protección de datos es un derecho autónomo y fundamental, por lo que demarca la principal diferencia, así lo señala Galvis “se identifica con la regulación centralista de mayor prevención y protección al derecho fundamental a la privacidad

de la información personal" (2018, p. 133). Además, se caracteriza por la prevención de las vulneraciones a este derecho a través del trabajo Estatal de cada Estado parte, señalando que:

> Se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas (Unión Europea, 2016, p. 3)

A su vez, el derecho al olvido surge en el RGPD como la facultad atribuible al sujeto de datos para eliminar la información correspondiente contenida en los servidores de internet, artículo 17, y señala la responsabilidad proactiva como el mecanismo que "busca que las empresas no sólo no incurran en incumplimientos, sino que también demuestren que están cumpliendo las disposiciones contenidas en la nueva regulación" (Agüero, 2019, p. 23).

En contraposición a este modelo proactivo, basado en un derecho fundamental y autónomo y dirigida a los gobiernos para implementar la mayor vigilancia posible sobre el tratamiento de datos automatizados y por ficheros, se encuentra el modelo estadounidense. Es un modelo basado en poca regulación sobre el TDP, así lo señala Agüero, al indicar que el modelo estadounidense tiene una regulación que "son de corto alcance y protegen principalmente, por no decir únicamente a los registros de salud y la información de crédito" (2019, p. 24). Entre las disposiciones en materia de protección de datos se encuentra la Ley Federal de Transacciones Crediticias Justas y Exactas, la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario. Para Galvis, este es un modelo que "responde a los requerimientos del nivel sectorial de carácter reactivo e individual de mayor confianza en el mercado" (2018, p. 133).

Estos dos modelos, ofrecen un panorama sobre la protección de datos en los distintos países, que si bien el modelo colombiano parece ser una mixtura de los dos por cuanto se presentan garantías de protección mediante principios, disposiciones legales y constitucionales. Estas aún se encuentran poco desarrolladas en un reglamento muy general por ser un campo relativamente nuevo.

Ahora bien, para el estudio del derecho comparado se abordan los casos de Alemania, desde la visión del marco jurídico europeo; México y Uruguay, como similares en materia de derecho latinoamericano, así:

Tabla 7. Legislación en materia de Habeas Data en Alemania, México y Uruguay.

| | |
|---|---|
| **Alemania** | Disposiciones relevantes:<br>-*Bundesdatenschutzgesetz,* se aprueba el RGPD el 27 de abril de 2017. |
| | Jurisprudencia relevante:<br>Apelación del Tribunal Federal de Justicia de Alemania, emitido el 23 de junio de 2020. confirma la decisión que acusó a la compañía Facebook de abuso de posición dominante a través de sus diferentes aplicaciones y red social, por vulnerar la protección de datos personales de los usuarios de Facebook al usar sus datos personales para proporcionar información para la eventual publicidad de las distintas empresas que contratan con la compañía, mediante herramientas de *Facebook*, como *Facebook Pixel*, *Facebook* analytics o los *plugins* (Bundesgerichtshofs, 2020). |
| **México** | Disposiciones relevantes:<br>- Artículo 6 Constitución de México, sobre habeas data.<br>- Ley General de Transparencia y Acceso a la Información Pública, reglamentó el artículo 6 de la Constitución de México.<br>- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.<br>- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México. |
| | Jurisprudencia relevante:<br>El fallo de constitucionalidad de la Suprema Corte de Justicia de la Nación, en el que se decidió sobre la invalidez de las normas demandadas por considerarlas limitantes al derecho de habeas data (Sentencia 29 318, 2020) |
| **Uruguay** | Disposiciones relevantes:<br>- Artículo 7 constitucional, sobre el derecho al honor, la libertad, la seguridad de las personas (Constitución de La República, 1967).<br>- Decreto 396 del 2006, la Ley 16.011 de 1988, sobre la acción de amparo de protección de habeas data.<br>- Ley 18.331 de 2008, sobre los derechos a "solicitar la rectificación, actualización, inclusión o supresión de datos personales que le corresponda incluidos en una base de datos" (SCHIAVI, 2017). |
| | Jurisprudencia relevante:<br>Fallo del Tribunal de lo Contencioso Administrativo de Urugay, que confirmó el acto administrativo emitido por la Unidad Reguladora y de Control de Datos Personales al considerar que la empresa BB violó la Ley 18.3331 de 2008, por realizar TDP sin la debida autorización de los titulares. (Sentencia Nº 350/13, 2013) |

*Nota:* *Exposición de la normativa en materia de Habeas Data en Alemania, México y Uruguay usando como referencia los países de Alemania, México y Uruguay, mediante la citación de normas y jurisprudencia en la materia. Por Yahaira Arévalo Aragón, 2020

# 2. Mecanismos De Protección De Datos Personales En Colombia Frente Al Entorno Digital (Redes Sociales Y Plataformas De Comercio Electrónico)

## 2.2. Administrativos

Como mecanismos de protección de datos personales, la ley 1266 de 2008 y la ley 1581 de 2012, contempla la petición o consulta y el reclamo, lo primero a determinar es que estas dos figuras se diferencian por cuanto la consulta es aquel mecanismo que permite al interesado obtener información acerca de los datos recolectados y almacenados en una base de datos; y el reclamo es el mecanismo por el cual el interesado ejerce su derecho al considerar que la información contenida en una base de datos debe ser corregida, actualizada, o bien, cuando considere que hay una falta a la norma de protección de datos.

Estos mecanismos tienen las siguientes formalidades según la ley en la que se encuentran:

Tabla 8. Mecanismos de protección de datos personales en el Decreto 1074 de 2015.

| **Mecanismo** | | **Ley 1266 de 2008 Artículos 14 a 16** | **Ley 1581 de 2012 Artículo 16** |
|---|---|---|---|
| **Consulta** | Interesado | Titular de la información o causahabiente | Titular de la información o causahabiente |
| | Dirigido a | Operador de datos | Responsable de tratamiento o Encargado de tratamiento |
| | Forma | Verbal, escrito, o por cualquier canal de comunicación, siempre que evidencie la consulta por medios técnicos | Medio habilitado por el responsable o encargado de tratamiento |
| | Términos | Primer término:<br>Diez (10) días hábiles contados a partir de la fecha de recibo de la misma.<br>*Si no es posible responder dentro del primer término, deberá dar respuesta dentro de los cinco (5) días hábiles siguientes al vencimiento del primer término. | Primer término:<br>Díez (10) días hábiles.<br>*Sino es posible responder en el primer término deberá dar respuesta dentro de los cinco (5) días hábiles siguientes al vencimiento del primer término. |

Tabla 8. Continuación

| **Reclamo** | **Interesado** | **Titular de la información o causahabiente** | **Titular o causahabiente** |
|---|---|---|---|
| | Dirigido a | Operador de datos, quien tendrá un término no mayor a dos (2) días para incluir la leyenda "reclamo en trámite" en la base de datos. | Responsable del Tratamiento o Encargado del Tratamiento quien tendrá un término no mayor a dos (2) días para incluir la leyenda "reclamo en trámite" en la base de datos. |
| | Forma | Solicitud escrita, debe contener: a quien va dirigida, identificación del titular, descripción de los hechos, dirección, documentos que pretenda hacer valer.<br>*Si la solicitud está incompleta, se requiere al interesado para que subsane su error. Si en un término de un (1) mes el interesado no realiza la corrección se entenderá desistida la reclamación.<br>*Si la información se encuentre en una fuente independiente, el operador debe dar traslado dentro de los dos (2) días hábiles siguientes a su recepción a la fuente, quien tendrá un término de diez (10) días hábiles para dar respuesta al operador. | Solicitud, debe contener: a quien va dirigida, identificación del titular, descripción de los hechos, dirección, documentos que pretenda hacer valer.<br>*Si la solicitud está incompleta, se requiere al interesado dentro de los 5 días siguientes a la recepción. Si en un término de 2 meses el interesado no realiza la corrección se entenderá desistida la solicitud.<br>*Si la solicitud está mal dirigida debe ser trasladada a quien corresponda dentro de los dos (2) días hábiles siguientes a su recepción. |
| | Término | Primer término:<br>Quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.<br>Segundo término:<br>Dentro de los ocho (8) días hábiles siguientes al vencimiento del primer término. | Primer término:<br>Quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.<br>Segundo término:<br>Dentro de los ocho (8) días hábiles siguientes al vencimiento del primer término. |

*Nota:* *Se exponen los mecanismos administrativos que contempla el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Adaptado de: (Decreto, 1074, 2015). Por Por Yahaira Arévalo Aragón, 2020

Cabe mencionar que tanto la ley 1581/12 como la ley 1266/08, señalan el mecanismo de la consulta como petición, no discrimina entre un término u otro, por lo que al consagrar los artículos mencionados la palabra consulta se deberá entender que esta se entiende a su vez como petición, de hecho, la Corte Constitucional al analizar la constitucionalidad de la norma encontró que esta figura comprendía los elementos fundamentales del derecho de petición y por ello no se tiene como un mecanismo alternativo, además estableció que este tiene una doble finalidad

> (i) permitir a los interesados elevar peticiones o solicitudes respetuosas a las entidades u organizaciones públicas o privadas que participan en el proceso de administración de los datos personales; y (ii) asegurar mediante la imposición de una obligación con cargo a las organizaciones requeridas, la respuesta y/o resolución de dicha petición, de manera oportuna, eficaz, de fondo y congruente con lo pedido. (Corte Constitucional, Sentencia C-1101, 2008)

Por otro lado, la ley contempla mayores formalidades en cuanto al reclamo, y a su vez, permite que los causahabientes ejerzan el derecho al habeas data, así lo señala el numeral 2 del artículo 20 del Decreto 1377/13, el literal a del artículo 13 de la ley 1581/12 y el literal a) del artículo 5 de la ley 1266/08.

En cuanto a la revocatoria de la autorización que permite el TDP, el Decreto 1377/13 señala únicamente al titular de los datos como el facultado para realizar la solicitud de la supresión de los datos personales o revocatoria de la correspondiente autorización de TDP, a su vez indica que esta solicitud debe tramitarse bajo las formalidades de un reclamo contenidas en la ley 1581/12. (Decreto1377/13, 2013)

En cualquier caso, si se trata de la revocatoria de la autorización que permite el TDP, o bien, de una consulta o reclamo, la norma prevé como mecanismo de protección de datos la instancia procedimental ante la SIC, que actuará una vez se verifique cumplido el requisito de procesabilidad contenido en el artículo 16 de la ley 1581/12, el artículo 9 del Decreto 1377/13 y el artículo 16 de la ley 1266/08.

La SIC como ente encargado de la vigilancia y control, podrá adoptar sanciones o imponer medidas correspondientes al establecer que se han incumplido con cualquiera de las normas de protección de datos. Sobre la imposición de sanciones por la SIC, las normas de protección de datos contemplan tres sanciones, estas son a) multa, b) suspensión de actividades relacionadas con TDP, c) el cierre temporal de las actividades de TDP y d) el cierre inmediato y definitivo de la actividad que implique el TDP. Por último, los criterios de graduación de las sanciones impuestas por la SIC a quienes incumplan con las normas de protección de datos van desde la dimensión del daño causado, el beneficio económico obtenido, la renuencia, la obstrucción a la investigación hasta la reincidencia de la infracción. (Ley 1581/12, 2012, art. 23-24; Ley 1266/08, 2008, art. 18-

19). Además, frente a las decisiones que den con ocasión de los mecanismos administrativos mencionados anteriormente, la ley faculta a la Delegatura para la Protección de Datos Personales, para resolver los recursos de reposición, revocatoria directa y de apelación que se presenten durante el proceso iniciado en las instancias de la SIC. (Decreto 4886 de 2011, art. 16)

Finalmente, en el comunicado que dio respuesta al derecho de petición radicado ante la Delegatura para la Protección de Datos Personales, el grupo encargado de la DIPDP señaló que los principales motivos por los cuales se activan los mecanismos administrativos ante la SIC son:

1. Infracción al deber y principio de seguridad, confidencialidad e integridad de la información, es decir, insuficientes e inadecuadas medidas técnicas, humanas y administrativas para garantizar seguridad a los datos personales.
2. Infracción al deber de obtener la autorización previa, expresa e informada del titular e informar lo que ordena el artículo 12 de la Ley 1581 de 2012
3. Infracción al deber de adoptar, implementar y desarrollar políticas de seguridad de la información y procedimientos para la recolección, almacenamiento, uso, circulación, supresión y disposición final de la información.
4. Infracción al deber de adoptar, publicar en sitio web, implementar y desarrollar una Política de Tratamiento de Datos Personales.
5. Infracción al deber de adoptar, publicar e implementar un Manual Interno de Políticas y Procedimientos para la atención de consultas y reclamos de los titulares.
6. Infracción al deber de conservar prueba de la autorización previa, expresa e informada otorgada por el titular.
7. Infracción al deber de garantizar al titular en todo tiempo el pleno y efectivo ejercicio del derecho de habeas data

(DIPDP, 2020)

### 2.3. Judiciales

Dentro de los mecanismos judiciales existentes para la protección de datos personales, se encuentran:

- Acción de tutela, se implementó con la promulgación de la Constitución Política de 1991 y se encuentra reglamentada por el Decreto 2591 de 1991. Este mecanismo judicial faculta a cualquier persona para reclamar ante cualquier juez del país la tutela de los derechos fundamentales consagrados en la Constitución política, cuando resultan vulnerados o amenazados por una acción y omisión tanto por autoridades públicas como por los particulares (Corte Constitucional, Sentencia C-483, 2008). La acción de tutela, además de ser un mecanismo subsidiario y residual, es de resolución inmediata y permite al afectado proteger lo antes posible sus derechos fundamentales.

  El artículo 15 constitucional al consagrar el derecho fundamental al habeas data permite que este instrumento judicial sea usado por el sujeto de derecho para proteger su autodeterminación informática cuando considere que su derecho se encuentra en amenaza o sea vulnerado, con la única particularidad que no cuente con otro medio más expedito para proteger su derecho, de allí su carácter subsidiario.

En cuanto a las formalidades de la acción de tutela, la Corte Constitucional ha señalado que esta no debe ser el resultado de tramites tediosos que impidan el acceso al mecanismo judicial del afectado en atención al principio de informalidad de la acción de tutela (Corte Constitucional, Sentencia C-483, 2008). Por lo tanto, la acción de tutela puede ser presentada en cualquier momento mientras se encuentre en peligro o haya sido vulnerado el derecho fundamental, esta debe ser resuelta en un término no mayor a diez (10) días y la decisión que ampara el derecho fundamental tiene efectos inmediatos, por consiguiente, el accionado tiene un término de 48 horas contadas a partir de la notificación de la decisión para dar cumplimiento con lo ordenado por el juez constitucional.

- **Demanda**

Por un lado, la demanda como mecanismo judicial se presenta en el caso que el titular de datos este ante una vulneración de su derecho a habeas data por la responsabilidad atribuida a la “fuente de la información” (Ley 1266, 2008, art. 16). El artículo 16 de la ley 1266, señala que la demanda una vez sea notificada, la fuente de información deberá comunicar al operador para que

> Dentro de los dos (2) días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro

> del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo en firme (Ley 1266, 2008, art. 16)

El mismo artículo faculta a la fuente de información a iniciar la demanda en contra del titular de datos por la obligación incumplida, cuando el titular proponga excepciones de mérito. Así, el proceso que se sigue es un proceso ejecutivo en materia civil.

A su vez, se encuentra la posibilidad de iniciar un proceso de responsabilidad civil contractual del habeas data financiero, al respecto la Corte Suprema de Justicia ha señalado que "La responsabilidad por violación del habeas data financiero es contractual, por cuanto las actividades de recolección, procesamiento y circulación de los datos del deudor, tienen origen en dos tipos de convenciones enlazadas entre sí" (Corte Suprema de Justicia, Sentencia SC3653-2019, 2019) Así, la responsabilidad contractual surge por una lado en un contrato de o de apertura de crédito contenidos en el artículo 1163 y el artículo 1400, respectivamente, del Código de Comercio, en su instancia inicial, o bien, en la autorización expresa que el titular de datos le confiere para su recolección y tratamiento en las bases de datos. Lo cierto es, que cual sea la figura aplicable, la demanda se resolverá bajo las disposiciones del Código General del Proceso.

### 2.4. Responsabilidad Demostrada (Accountability)

El artículo 26 del Decreto 1377/13 señala como deber de los responsables del TDP, demostrar ante la SIC, cuando esta lo solicite, la implementación de medidas apropiadas y efectivas para la protección de datos personales consagradas en la ley 1581/12 (Decreto 1377/13, 2013). Esta facultad legal asignada a la SIC de promover, cuando considere necesario, petición dirigida a cualquier empresa pública o privada que realice TDP a través de base de datos o archivos, permite fortalecer la función de control y vigilancia asignada a la SIC. Así, cuando la SIC lo considere, el responsable de TDP deberá demostrar:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares

(Decreto 1377, 2013, art. 26)

La responsabilidad demostrada tiene sus antecedentes en las directrices señaladas por la OCDE en 1980, esta obligación a cargo del responsable de TDP se fundamenta a su vez en la obligación de implementar políticas internas eficaces para proteger los datos personales. Para la SIC, para que el programa en mención sea efectivo debe contener al menos "políticas que (I) respondan a los ciclos internos de gestión de datos de la organización y (II) generen resultados medibles que le permitan probar ese grado de diligencia espacial" (SIC, 2020, p. 8)

A su vez, el artículo 27 del Decreto 1377, señala que las políticas internas de las empresas que realicen TDP debe contener al menos:

> Una estructura administrativa proporcional a la estructura del responsable para implementarlas, […] 2. Adopción de mecanismos internos para poner en práctica las políticas que incluyan herramientas de implementación, entrenamiento y programas de educación, 3. la adopción de procesos para la atención de reclamos y consultas de los titulares. (Decreto 1377/13, 2013, art. 27)

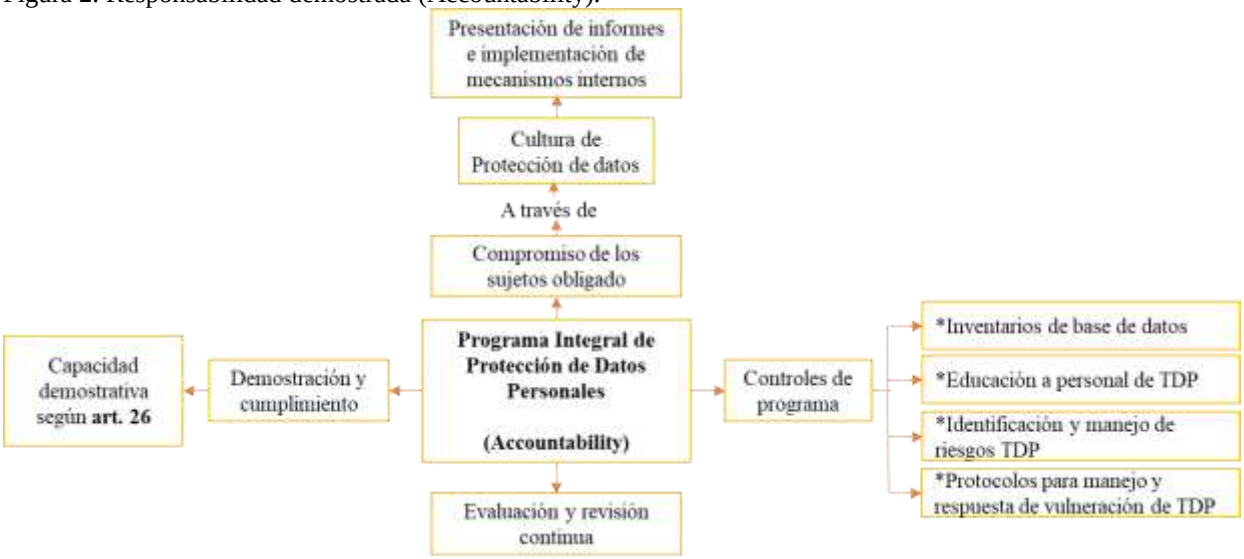
De igual forma, mediante Circular emitida por la SIC el 5 del 10 de agosto del 2017, ordenó:

> Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, Los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia. (Citado por SIC, 2019a)

Esta obligación permite diseñar y promover la implementación de políticas de protección de datos efectivas no solo en su creación, sino hasta su desarrollo, la idea principal de la responsabilidad demostrada a cargo de los responsables de TDP es mantener un sistema de alto nivel de protección efectivo, mediante el estudio y evaluación constante incluso de las políticas ya implementadas, no se trata de solo crear políticas para cumplir con un mandato legal, estas políticas

deben estar en constante control y evaluación por parte de los responsables de TDP; ello no implica que la SIC prescinda de sus funciones como ente de vigilancia y control a través de la Delegatura de Protección de Datos, al contrario, la función de protección de datos se ve reforzada por la constante posibilidad de exigir en cualquier comento a los responsable de datos demostración de la efectividad y evaluación de sus políticas de protección de datos, lo que se traduce en un sistema preventivo, proactiva y de un nivel adecuado de protección de datos.

Figura 2. Responsabilidad demostrada (Accountability).




*Nota:* * Elementos esenciales a tener en cuenta por quienes realizan TDP para la creación e implementación del Programa Integral de Protección de Datos Personales y el abordaje del principio Accountability, según SIC, Guía para la Implementación de Responsabilidad Demostrada (Accountability). (2015). Por Yahaira Arévalo Aragón, 2020

Así, Accountability se presenta como un mecanismo de protección de datos a nivel interno, ordenado por la ley 1581/12 y el decreto 1377/13, que al facultar a la SIC solicitar en cualquier momento que los encargados y operadores de TDP, tengan medidas y políticas internas eficientes y adecuadas, en todo momento, para asegurar la protección de datos personales. Este mecanismo puede ser ejercido en cualquier momento, a solicitud de la SIC, sobre las exigencias contenidas en el artículo 26 del decreto 1377. Como ejemplo se presenta el reciente comunicado emitido por la SIC en el cual señala que inició de "oficio una actuación administrativa con el propósito establecer si ZOOM VIDEO COMMUNICATIONS INC, cumple o no con la regulación colombiana relativa a los principios de seguridad, acceso y circulación restringida" (SIC, 2020d, par. 1)

# 3. Desafíos De La Protección De Los Datos Personales En El Entorno Digital

## 3.1. Big data y la aplicación de minería de datos

La recolección masiva de datos en los entornos digitales que son procesados y tratados usualmente son almacenados en bases de datos. El gran tráfico de datos, es decir, su tratamiento masivo permite que hoy se hable de *Big Data*, sin embargo, este término es propio del campo genético o astronómico, donde necesitan codificar cantidades de datos muy extensas. En cuanto a la cantidad de datos que deben ser obtenidos para ser considerados como big data entiende como tal, desde unas decenas de terabytes en adelante esta consideración no es una cifra exacta, de hecho, big data se refiere a grandes cantidades de almacenamiento y tratamiento de datos sin especificar una cantidad exacta. Ahora, en cuanto a la forma en que son almacenados los datos durante su tratamiento en el entorno digital, se puede producir mediante datos estáticos, almacenados usualmente en formato de ficheros o bien, los datos dinámicos, producidos continuamente y por tanto su recolección no es permanente (Casas, Nin & Julbe, 2019)

El impacto del análisis masivo de datos ha conducido a los Estados a regular la materia para evitar la vulneración a la protección de datos personales e incluso se ha planteado la posibilidad de que la legislación actual puede verse como ineficiente frente a los constantes desarrollos de tecnología para el tratamiento masivo de datos personales. Así lo señala, Gayo “aplicados al tratamiento de datos personales, estos principios ya no son eficientes si pensamos en la realidad actual y en el futuro” (2017, p. 2) acertadamente este autor argumenta la limitación e inflexibilidad de las normativas estatales al referirse en sus disposiciones a cantidades pequeñas de datos personales. Los big data necesitan una regulación eficiente pero no limitativa, se reconoce la importancia y necesidad de los big data para el desarrollo de la economía y el futuro de la tecnología. Big data, tiene dos fases, una fase de identificación, recolección y almacenamiento, y una segunda fase en la cual se aplican las herramientas de análisis mencionadas como el KDD.

Ahora bien, la minería de datos es una de las herramientas más usadas para el análisis y estudios de datos incluso en el entorno digital, puesto que puede analizar datos contenidos en diferentes formatos y no los usuales de combinaciones numéricas binarias o caracteres como lo hacían los lenguajes como *SQL* o *OLTP*, estas herramientas son consideradas parte del proceso *Knowledge Discovery in Databases* (KDD) mediante el cual se extrae conocimiento a partir de diferentes mecanismos de análisis de datos recopilados en una base de datos. La minería de datos, hace parte de una de las fases de KDD y "está constituido por una o más de las siguientes funciones, clasificación, regresión, clustering, resumen, recuperación de imágenes, extracción de reglas" (Riquelme, Ruiz, Gilbert, 2006, p. 13)

Durante esta fase la posibilidad de generar afectaciones a la protección de datos personales contenidas en las bases de datos debería ser un factor importante a la hora de realizar estas prácticas, teniendo en cuenta los procesos que se han de realizar. Cada uno implica el análisis, agrupación, categorización, nuevos almacenamientos, entre otros. Cada una de estas interfases representan riesgos potenciales para el TDP. Además, el empleo de actividades automatizadas mediante redes neuronales, arboles de decisión, algoritmos, por ejemplo, puede degenerar la protección de datos al desempeño positivo o negativo de la práctica automatizada. Para Gayo, durante el TDP se deben evaluar la intervención de cada uno de los actores de esta actividad, desde quien realiza el proceso de recolección de datos, quien los analiza o los trata, hasta quien los usa, cada uno de estos estamentos durante la actividad de TDP implica ir más allá de cuestiones de autorización y finalidad del TDP, para remitirse a la responsabilidad demostrada como principal mecanismo de protección de datos *ex ante* y *ex post* (Gayo, 2017).

### 3.2. Implementación de Inteligencia Artificial (IA)

La cuarta revolución industrial, la llegada de nuevas tecnologías que potencian la capacidad humana y mejora la interacción con el mundo, ha generado entre otras herramientas el surgimiento y popularidad de la Inteligencia Artificial (IA), esta ciencia limita en el campo de las ingenierías, su creación, diseño e implementación ha generado resultados positivos en la industria permitiendo que las tareas sean más eficientes, y a su vez, se vea fortalecida la economía.

En el año 2017 el Instituto de Transformación Digital de Capgemini realizó una encuesta entre los meses de marzo y junio del mismo año donde pudo concluir que el "75% de las empresas que usaron inteligencia artificial elevaron un 10% sus ingresos" (La Vanguardia, 2017, par.1). En el año 2018, el Ministerio de Tecnologías de la Información y Comunicaciones (Min Tic, par. 1) señaló que el 1.8 % de empresas colombianas usan Inteligencia artificial y a su vez señaló "Para economías emergentes como la colombiana, el potencial de crecimiento es gigantesco. Expertos mundiales han coincidido y han definido esta tecnología como una forma de potencializar el trabajo humano" (Min Tic, 2020, par. 2)

IA se presenta como una obligación para las empresas colombianas como potenciación de sus ingresos y por ende de la economía. IA funciona generalmente a través de algoritmos que permiten tomar decisiones a partir de los datos almacenados y recolectados por bases, los cuales son ejecutados mediante memoria reactiva (Business Insider, 2019) o bien, mediante una memoria limitada que disminuye la capacidad de registro de datos pero focaliza actividades determinadas, por ejemplo las cámaras más actuales incorporadas en los móviles que a partir de datos ingresados previamente, establece parámetros fotográficos que le permite conseguir al consumidor mejores imágenes (Business Insider, 2019).Sin embargo la IA puede usar otras tecnologías como el aprendizaje automático Según una publicación de Forbes Colombia, "No tener una estrategia de inteligencia artificial en tu modelo de negocio para los próximos 2 años es el equivalente a no tener un sitio web en el año 2000" (Vega, 2020, par.14)

### 3.3. Consumidor algorítmico.

La IA se caracteriza por su constante evolución, no es un concepto estático por lo que a diario se revoluciona y propone nuevos retos a las tecnologías y los impactos que esta genera. Un nuevo reto que ha surgido a partir de la implementación de IA y que se presenta como ejemplo a esta ciencia, es el consumo a partir de algoritmos. El término consumidor algorítmico fue dado a conocer por Michal Gal y Niva Elkin-Koren, en su artículo, señalan que las próximas generaciones de consumidores estarán conducidos o determinados por agentes digitales a través de algoritmos que adoptaran transacciones que antes realizaban los mismos consumidores (Gal & Niva, 2017).

Estas nuevas generaciones de consumidores están mediadas por agentes digitales que influirán y casi tendrán la capacidad de tomar las decisiones de los consumidores a los que asisten, además, provocará que aspectos de la economía como la demanda en el mercado, las estrategias usadas para la comercialización de productos y servicios, los términos en los que se llevan a cabo los comercios e incluso determinaría la demanda de los productos de los proveedores (Gal & Niva, 2017).

Entonces, si se media un agente digital que utilice IA para realizar algoritmos que influyan en las transacciones que realiza un consumidor promedio, esto podría afectar entre otras cosas su capacidad de elección y autonomía limitando el conocimiento, por ejemplo, que debería tener sobre cada una de las transacciones que relevaría en este nuevo agente digital. Además, para dar cumplimiento con el cometido de un consumidor algorítmico, el agente digital deberá contar con una fuente para recolección de datos personales que deberán ser almacenados en bases de datos de la empresa o compañía que esta ofreciendo esta tecnología. Lo anterior, presentaría mayor riesgo para la protección de TDP, a su vez, implicaría un nuevo reto para los entes de control y vigilancia.

IA en su interacción con los usuarios de un producto o servicio siempre va a implicar el TDP, lo que no se traduce precisamente en una vulneración a los datos personales de los usuarios, al contrario, no se busca limitar IA sino promover el uso de mecanismos y protección durante el TDP. Uno de los aspectos que más atención requiere es sobre quien recae la responsabilidad del TDP señaladas en la Ley 1581 o en la Ley 1266, para que una tecnología de IA sea eficiente se requiere muchos actores que se encargan de diferentes ámbitos pero que en todos son necesarios el TDP. Además, si la IA usualmente realiza acciones automatizadas, se debe determinar cuál es el papel del sujeto de derechos mediante el ejercicio de los mismos. Al respecto, es preciso remitirse a los Estándares emitidos por la RIPD, en el cual se consagro la posibilidad del titular de los datos de solicitar la intervención de un humano cuando un programa de IA que tome decisiones individuales automatizadas, realice una acción con la cual el titular de datos no se encuentre de acuerdo, es decir, se establece la posibilidad de impugnar la decisión de la IA ante un humano (SIC, 2019)

De igual forma, es importante que la empresa que utilicen IA, o en el caso de los consumidores algorítmicos, tengan la oportunidad de obtener un producto o servicio de IA,

mediado por la *Privacy by Desing and by Default* esta expresión se refiere a la implementación de estándares de protección de privacidad en la IA desde su diseño o bien por defecto. Es una medida atribuida al principio de responsabilidad demostrada o Accountability, según la SIC, "Al incrustar la privacidad desde el diseño, se está buscando garantizar el correcto tratamiento de los datos utilizados en procesos de inteligencia artificial, incluso antes de la materialización de los riesgos" (SIC, 2019) De hecho, aunque se tiene la concepción que al ser IA, y realizar prácticas automatizadas tienen un margen de error casi nulo, lo cierto es que por ejemplo, en el caso de la IA a través de algoritmos, estos pueden presentar riesgos inherentes como lo son sesgos durante los datos de entrada, es decir, una toma parcializada de datos que influyen en su calidad; también puede presentar patrones que afectan el desarrollo del algoritmo como lo son los sesgos en la lógica de programación o en el caso de una falla en la codificación (SIC, 2019)

Sin embargo, actualmente Colombia no ha regulado de manera expresa las tecnologías y herramientas usadas a través de IA, en las leyes 1581/12 y 1266/08, no se menciona la IA como posible ámbito a regular, para el caso, Martínez señala "dentro de la actual regulación colombiana no se contempla el uso de las nuevas herramientas de IA mediante las cuales se recolectan datos, como cookies y el web crawling" (2019, p. 1)

### 3.4. El perfilado de datos (*Profiling*)

Cada usuario de internet tiene un perfil virtual, las apps redes sociales, plataformas de *e-commerce*, entre otros entornos digitales crean perfiles a partir de la interacción de los usuarios con los medios digitales. Un perfilado de datos se realiza a partir de la información que el usuario comparte, hace público, o bien, permite su acceso en el entorno digital.

En principio, una actividad de perfilado de datos no debería representar mayor problema si cuenta con la autorización del titular de datos, y que este conozca las finalidades sobre las que se realiza TDP a sus datos personales. Sin embargo, usualmente se presentan casos de *function deep* o usos encubiertos; estos usos representan el principal problema para la protección de datos personales en el entorno digital. La incapacidad de cada titular de datos, usuario de un medio digital, que autorice su TDP para determinados fines, conocidos, y que sus datos se vean

implicados en TDP diferentes, extensivos, inadecuados, afectando sus derechos. Para ejemplificar un poco lo propuesto, se toma los datos de la SIC que indica que, en el año 2017, se presentaron 610 denuncias entre las que se encuentra "utilización de información de personas con fines de mercadeo sin la autorización del titular" (citado por Galvis, 2018, p. 135)

Casos como la serie de la plataforma *streaming* Netflix, *House of cards,* fue el resultado de la intervención de IA y algoritmos a partir de la interacción de los usuarios en esta plataforma lo que llevo a la empresa a tener un éxito mundial en mencionada serie. De igual manera, el tan sonado caso *Cambridge Analityca* y las elecciones estadounidenses del año 2016, e incluso casos más actuales como las investigaciones que está adelantando la SIC a las empresas *Zoom Meeting* y *Tik Tok Pte Ltda*, plataforma de videoconferencia y red social respectivamente; estas investigaciones se adelantan en atención a la implementación del principio de responsabilidad demostrada por parte de las empresas en mención, su eficiencia frente a la protección de datos personales de los usuarios colombianos.

Si bien, estos dos últimos casos mencionados corresponden a medidas preventivas, pues aún no se ha concluido que se hayan incumplido las obligaciones y regulaciones consagradas en la normativa de protección de datos colombiana, lo cierto es que durante un TDP se pueden emplear técnicas que permiten el perfilado de datos personales con usos comerciales o publicitarios.

A continuación, se exponen las siguientes técnicas:

### 3.5. Corredores de datos (data brokers).

Los *data brokers* o corredores de datos, tienen la finalidad de recolectar y acumular los datos personales, para ofrecer servicios a partir de los mismos mediante su tratamiento (Gonzales, 2019; Gayo, 2017) usualmente estos servicios pretenden un lucro sobre el uso de los datos personales del titular de datos que actúa como usuario en un entorno digital. Estas figuras permiten que las empresas y compañías potencialicen sus ofertas al permitir llegar al comprador indicado la información indicada. El uso de los data brokers ha cobrado especial importancia porque además de dirigir la publicidad al público adecuado, permite que las empresas enfoquen sus esfuerzos en

este grupo poblacional previamente seleccionado por el data brokers, reduciendo los costos en otros estudios y análisis, y obteniendo mayor precisión en su publicidad.

La especialidad de los data brokers es usar los datos contenidos en fuentes como son gubernamentales, censos, empresas de seguridad social, las licencias profesionales, e incluso recolectan datos a partir de *webcrawlers*, que usa los buscadores como Google o Yahoo, hasta las páginas de LinkedIn, Facebook, Twitter, e incluso actividades comerciales que son llevadas a cabo mediante ventas por catálogo, el uso de tarjetas frecuentes, entre otras (Gonzales, 2019) Técnicamente un *webcrawlers* es un metabuscador que usa otros buscadores o bien, usa información a partir de páginas, redes sociales, u otros medios del entorno digital para arrojar sus resultados. Entonces, cada red social, plataforma de e-commerce, Marketplace, contrata con empresas de servicios de *data brokers* o *webcrawlers*, para potenciar la publicidad de sus productos y servicios. Ejemplo de ello, es *Experian Information Solutions*, mediante *Expirian Colombia S.A.* ofrece servicios de información crecidita a través de Data Crédito. A su vez, la empresa Acxiom asociada con empresas como Facebook, Pinterest, ebay, PayPal Media Network, IBM, entre otras.

Ahora bien, respecto a los efectos que tienen estos análisis de datos personales sobre los usuarios en el entorno digital, Pew Research Center, realizó una encuesta a un grupo seleccionado de usuarios de Facebook, entre otros sobre el impacto que tiene la categoría *You ad preferences*, affinities y multicultural affinity, a partir de ello, se determinó que el 74% de los encuestados no tenían idea sobre la existencia de estas categorías preestablecidas de Facebook, a su vez, encontraron que el 51% señalo no sentirse comodos con las catergorizaciones que realiza la empresa a partir de la interacción en la red social (Hitlin & Rainie, 2019)

### 3.6. Cookies y Tecnologías de rastreo

Las Cookies son el factor clave para que las empresas que ofrecen servicios y productos en el entorno digital puedan mejorar el impacto en los usuarios y posibles compradores. Las cookies presentan variaciones técnicas de acuerdo al medio usado por el usuario en el entorno digital. Así se pueden distinguir las cookies permanentes, aquellas que son instaladas en los dispositivos usados para acceder a los diferentes medios del entorno digital; cookies de sesión, se activan al

momento de iniciar sesión usualmente en plataformas de e-commerce o Marketplace; cookies de publicidad, preferencia, entre otros.

Cada empresa instala sus propias cookies para tener una mayor afinidad con el usuario al que desean ofrecer su producto o servicio. Ello implica que, la cantidad de cookies que pueden ser instaladas en el disco duro del ordenador, y aceptadas por un usuario regular en el entorno digital dependerá de la navegación que realice en el mismo, la cantidad de páginas web, redes sociales, Marketplace que utilice. Esto fomenta la creación de su perfil digital y mejora la atención que ofrece la empresa frente a sus productos. A su vez, las cookies facilitan la tarea a los data brokers, al momento de recolectar y almacenar datos para luego ser proporcionados a las empresas que han contratado sus servicios.

De igual manera, las cookies son fomentadas a partir de las demás tecnologías de rastreo que se hacen presente durante el periodo de interacción del usuario en el entorno digital. Una cookie se guarda en un formato de texto para ser usado por el medio que la proporcionó luego, la cookie es nombrada con un ID, se le asigna un valor numérico - alfabético, se determina el dominio de acceso, tamaño, y señala a su vez la fecha de creación y expiración. Usualmente las cookies pueden ser identificadas en la configuración de los buscadores o navegadores que tenga en uso el usuario. A pesar que las cookies son piezas de información necesarias para el correcto y eficiente funcionamiento de cualquier medio del entorno digital, en ocasiones representa un problema para los usuarios y titulares de datos, puesto que, sin tener conocimiento, permiten el acceso a datos suministrados. El problema principal podría radicar en las cookies usadas por terceros, caso de los data brokers.

En cuanto a las clases de tecnología de rastreo, Hoofnagle, Soltani, Good & Wambach señalan que estas se pueden clasificar en dos clases, “Las primeras, se guardan en el equipo terminal como http cookies, E-tags, y Flash cookies. El segundo tipo identifica las particularidades técnicas de los dispositivos para individualizarlos y se denomina “huella digital de dispositivo” o fingerprinting” (como se citó en González, 2019, pp. 216-217) Respecto a la primera clase de tecnología de rastreo, González señala la dificultad para decidir sobre los aspectos de privacidad y conceder permisos por parte de los usuarios; respecto a la segunda clase tiene la capacidad de

recolectar características de los dispositivos identificando batería, imagen entre otros (González, 2019)

### 3.7. Identificadores de publicidad.

Por último, los identificadores de publicidad facilitan el acceso a los datos personales que permiten identificar el comportamiento del usuario en el entorno digital. En el caso de los dispositivos móviles, la activación de los identificadores de publicidad, usualmente, se hace de manera automática, ello depende del tipo de sistema que tenga el dispositivo. Sin embargo, para su activación o desactivación solo se requiere acceder a la categoría de configuración del móvil e inhabilitar los permisos concedidos para mejorar la segmentación de la información que se recibe.

El impacto del internet de las cosas en la actualidad conlleva al replanteamiento de las normativas que regulan la protección de datos personales del usuario que experimenta a través del entorno digital. El caso de los dispositivos móviles, Google señala que

> En las aplicaciones móviles no hay cookies, sino que, en su lugar, Ad Manager utiliza identificadores que facilita el sistema operativo del dispositivo móvil y que el usuario puede cambiar. Los ID de publicidad habituales son AdID (Android) e IDFA (Apple). Con estos ID, los desarrolladores y los profesionales del marketing pueden hacer un seguimiento de la actividad con fines publicitarios, así como mejorar las funciones de servicio y segmentación (Google, 2020, par. 1)

Desde una primera lectura a esta indicación de Google, no se presenta mayor preocupación, sin embargo, al tener los ID de publicidad acceso a los datos personales del titular de datos por medio de su teléfono móvil, incluso cuando el usuario no sea realmente consciente de haber permitido o habilitado esta función, se replantea la idea si se está cumpliendo con el principio de la finalidad del TDP, o con la obligación de la autorización esto es, " consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales" (Ley 1581/12, 2012, art. 3)

A su vez, respecto a la segmentación de la cual comunica Google, es pertinente hablar nuevamente de la función del perfil digital y la capacidad de las redes sociales o Marketplace, por

ejemplo, para enviar la información adecuada, al usuario adecuado, a pesar de que ello implique la segmentación de la misma a partir, incluso de datos personales de tipo sensible.

Para la SIC, “cualquier gestión de marketing, mercadotecnia o publicidad debe ser respetuosa de, entre otras, lo que ordena el artículo 15 de la Carta Política” que, a su vez, fue desarrollada por la Ley 1581 del 2012. El reto por ejemplo de los identificadores de publicidad es que las empresas implementen la responsabilidad demostrada en cada una de sus actividades, una implementación continua y minuciosa, que, en todo caso permita garantizar medidas adecuadas “aquellas ajustadas a las necesidades del Tratamiento de datos. Y “efectivas” son las que permiten lograr el resultado o efecto que se desea o espera” (SIC, 2019b)

### 3.8. Apps sociales y comercio digital

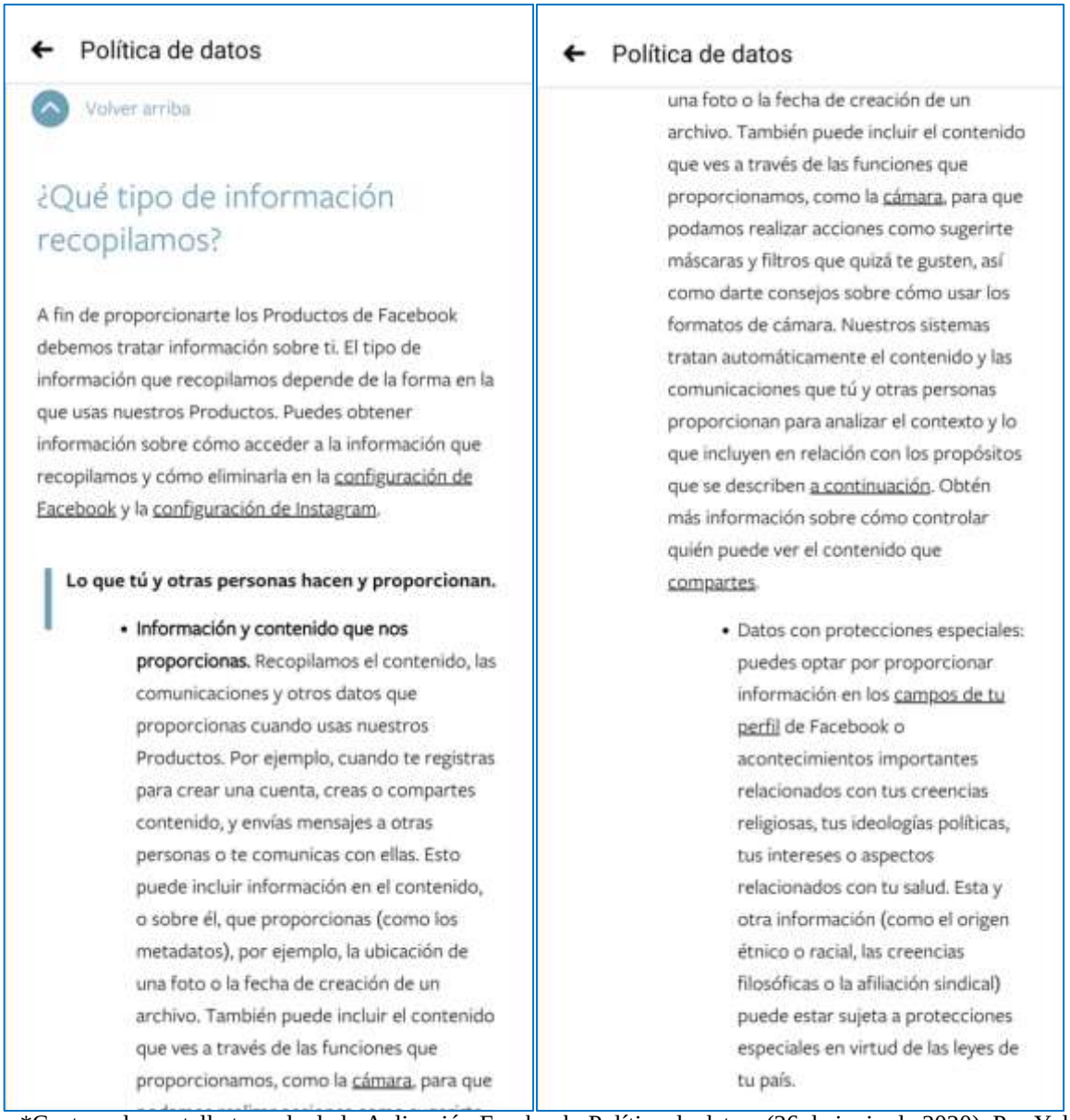
Desde las aplicaciones que permiten el acceso a redes sociales, buscadores, portales de contacto, videoconferencias, pagos en línea, entre otros. Cada una de estas aplicaciones, sin importar la empresa que la genere, recolecta, almacena y realiza tratamiento de datos personales, en mayor o menor medida. Cada vez que se descarga una nueva App en el dispositivo móvil, esta solicita permisos de accesos, habilita o deshabilita funciones, entre otras. Según el último informe de AppsFlayer, en el primer periodo del año 2020, las apps más descargadas son las dedicadas a prestar servicios de domicilio y salud, en Colombia, se presentó un aumento en las aplicaciones de Zoom, Tik Tok, Hangouts Meet, Microsoft Teams y Houseparty (citado por La República, 2020)

El primer periodo del año 2020, la humanidad se vio sometida a un régimen de cuarentena, por lo cual el aumento de la experiencia en el entorno digital aumentó significativamente. Las tareas diarias se volvieron digitales, y ello implicó un mayor uso de apps, que antes no se encontraban descargadas en los dispositivos móviles.

Ahora bien, cada vez que se descarga una nueva app en el dispositivo móvil, el usuario y titular de datos tiene la oportunidad de informarse acerca de los TDP a los que se verán sometidos sus datos para el correcto y eficiente funcionamiento de la app. Sin embargo, en ocasiones se presentan usos excesivos, que delimitan el principio de la proporcionalidad consagrado en

disposiciones como los Estándares de la Red Iberoamericana para la Protección de Datos Personales, o incluso el Reglamento General de Protección de Datos Personales.

Figura 3. Política de datos de Facebook.

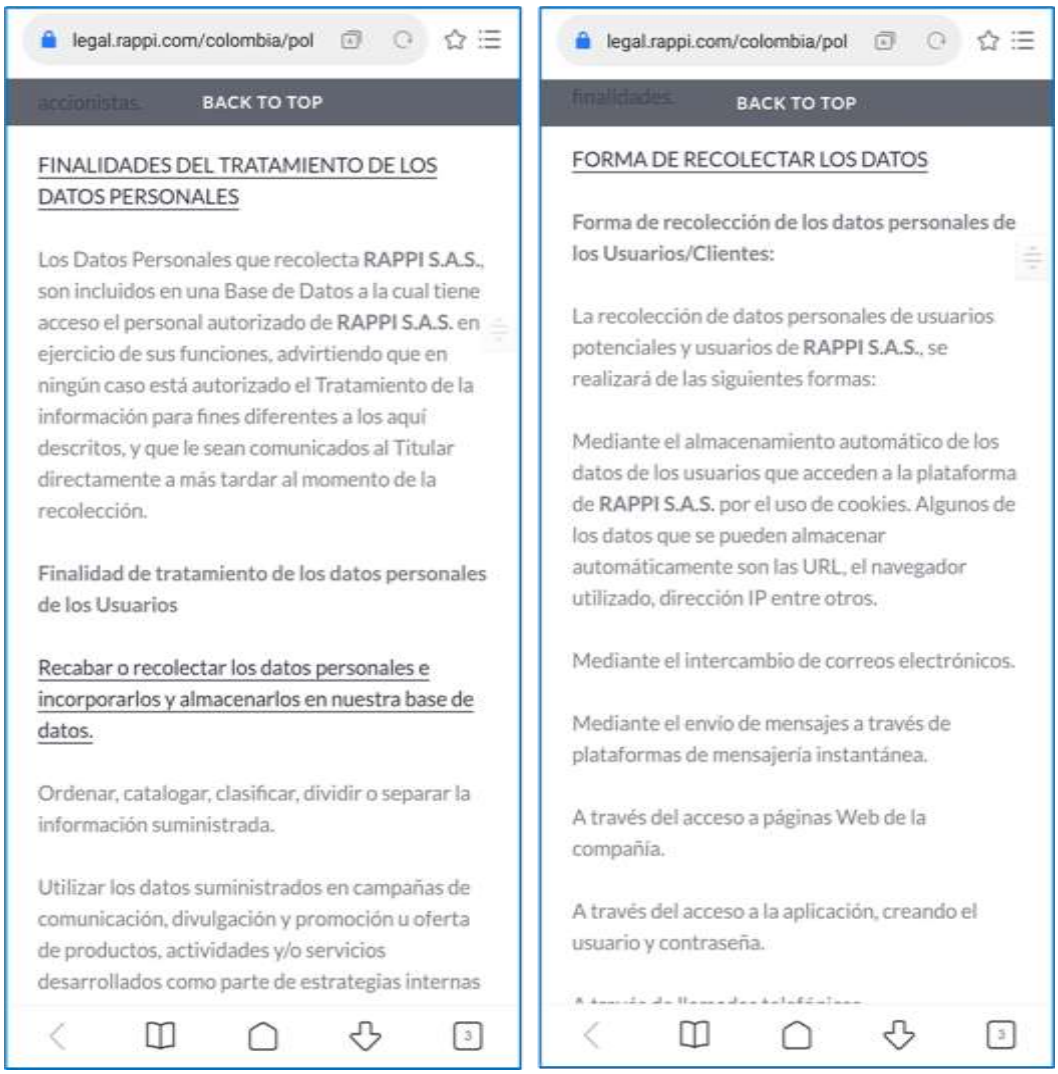



*Nota*: *Captura de pantalla tomada de la Aplicación Facebook. Política de datos. (26 de junio de 2020). Por Yahaira Arévalo Aragón, 2020

Facebook, cuenta con una Política de Datos estándar, que incluye sus servicios Facebook, Messenger, Whatsapp, Instagram, Direct, Boomerang, entre otros. En la Política de datos señalada, Facebook menciona un amplio uso y TDP. Además, señala que comparten información con “las Empresas de Facebook como externamente con nuestros socios y con las personas que te conectas

y compartes contenido en todo el mundo, de conformidad con esta política" (Facebook, 2020, par. 1)

Figura 4. Política de datos Rappi.




*Nota*: *Captura de pantalla de la política de datos de la empresa colombiana Rappi S.A.S. obtenida a partir de la página oficial de la empresa (26 de junio de 2020). Por Yahaira Arévalo Aragón, 2020

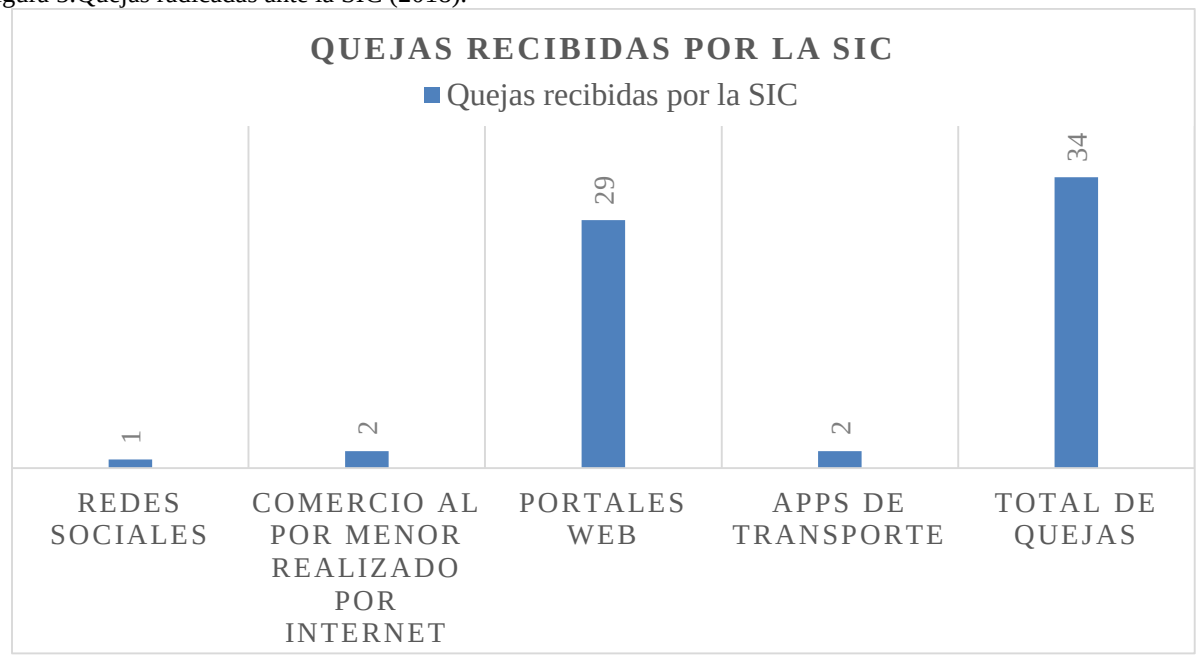
De igual forma, la empresa Rappi S.A.S., proporciona su política de datos a través del link de acceso, en la cual informa a sus usuarios que su política se acoge a la normativa colombiana Ley 1581 de 2012, hace una pequeña transcripción de las disposiciones consagradas en la ley y a su vez expone a sus usuarios la forma en que recolecta los datos y la finalidad para lo cual son recolectados.

Es preciso citar el caso de la app de citas Tinder, en esta app, se usa el clic de match para mejorar los resultados y búsquedas de los usuarios para conseguir pareja en línea, hasta allí parece excelente. Sin embargo, los algoritmos e inteligencia artificial usados por Tinder, además de mejorar sus resultados de match, utiliza datos personales de sus usuarios, los vende e incluso los categoriza mediante profiling identificando rangos de belleza para mejorar los resultados de los match, esto es conocido como segregación. Es un claro ejemplo de afectación a datos sensibles, pues perfilan a las personas a partir de los datos biométricos, mediante las selfies o fotografías que publican voluntariamente los usuarios en la app sin conocer a cabalidad los usos de sus datos personales. Esto desata nuevamente la discusión sobre la paradoja de la privacidad, qué tan dispuestos están los usuarios del entorno digital a sacrificar sus datos personales para poder usar las diferentes los servicios y productos que las empresas prestan.

## Resultados

A partir de la respuesta dada el 17 de julio de 2020, por la DIPDP se obtuvo que la cantidad de quejas presentadas por vulneración de PDP, en el año 2018 fueron:

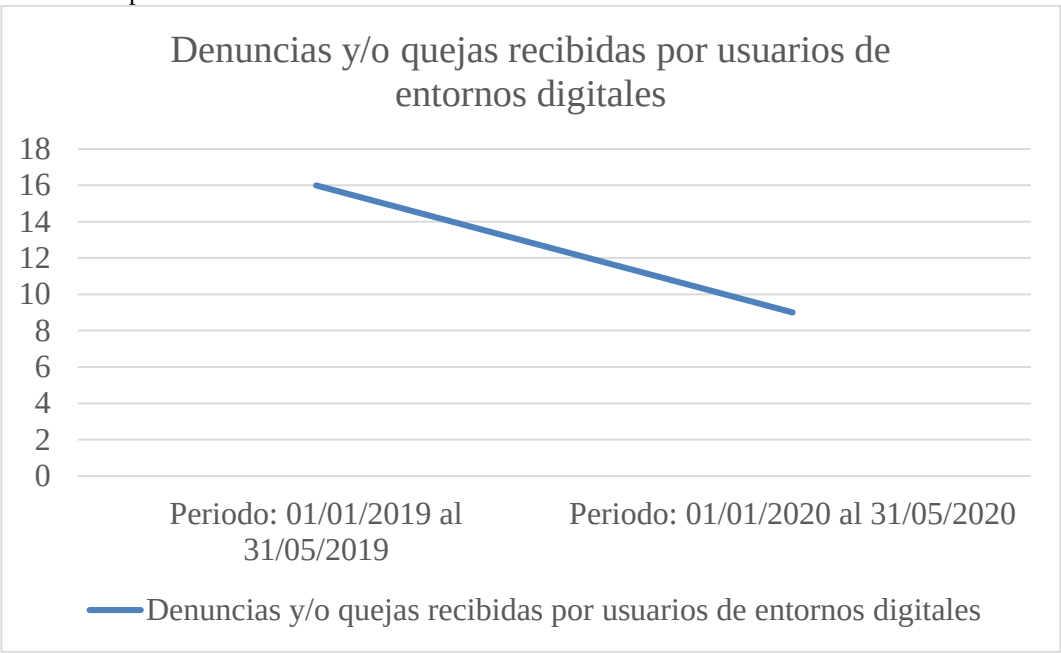
Figura 5.Quejas radicadas ante la SIC (2018).




*Nota*: *Gráfica realizada a partir de la respuesta al derecho de petición dirigido a la SIC. Fue emitida por la Dirección de Investigación de Protección de Datos Personales de la SIC. (17 julio 2020). Por Yahaira Arévalo Aragón, 2020

En cuanto a las denuncias y/o quejas recibidas por las SIC en el primer periodo del año 2019 y del año 2020, la SIC señaló que se presentaron 16 y 9 denuncias respectivamente, para un total de 25 denuncias recibida durante el período 01/01 al 31/05 de 2019 y 2020.

Figura 6. Denuncias presentadas ante la SIC.




*Nota*: *Gráfica realizada a partir de la respuesta al derecho de petición dirigido a la SIC. Fue emitida por la Dirección de Investigación de Protección de Datos Personales de la SIC. (17 julio 2020). Por Yahaira Arévalo Aragón, 2020

En cuanto a la cantidad de sanciones presentadas anualmente en los años 2018 y 2019, la SIC señalo que se presentaron un total de 4 sanciones, correspondientes a la vulneración de la disposición contenida en el literal a y d del artículo 17 de la Ley 1581 de 2012 y b y c del artículo 17 de la Ley 1581 de 2012 respectivamente. Respecto al año en curso, señaló no haber sanciones en firme, pero si menciono la reciente investigación en contra de Facebook por el cumplimiento del principio de Responsabilidad Demostrada (Accountability).

Figura 7. Denuncias presentadas, por el literal a y b del artículo 17, ley1581/12.


*Nota*: *Gráfica realizada a partir de la respuesta al derecho de petición dirigido a la SIC. Fue emitida por la Dirección de Investigación de Protección de Datos Personales de la SIC. (17 julio 2020). Por Yahaira Arévalo Aragón, 2020

No obstante, la SIC, a través de su página oficial de Instagram realizó una publicación acerca de los Logros de la Delegatura para la Protección de Datos Personales, en el periodo comprendido entre el año 2018 y el año 2020, en la cual señaló los siguientes resultados:

- Se presentaron 23.252 solicitudes ciudadanas respecto a temas sobre TDP.
- Se realizaron 135 multas por más de 12 mil millones de pesos
- Se emitieron 1.642 órdenes administrativas para mejorar medidas de seguridad, suprimir información falsa.

(SIC, 2020)

De igual forma, la DIPDP señaló que, si bien a la fecha de la respuesta al derecho de petición no existían sanciones en contra de alguna red social, si mencionó una orden emitida por la SIC dirigida hacia la compañía estadounidense Facebook, en la cual le solicitaban describir y demostrar si estaba cumpliendo adecuadamente con la PDP contemplada en la legislación colombiana. (DIPDP, 2020) Esta orden se ejecutó sin base en denuncia o queja propuesta por usuario alguno de la red social, sino de oficio, bajo el principio de responsabilidad demostrada que como se expuso faculta a la SIC para exigir a quienes realicen TDP demostrar el cumplimiento del

marco normativo de PDP en Colombia. De hecho, en las cifras publicadas por la SIC en la página oficial, se señala un total de 1.642 ordenes administrativas impuestas entre el año 2018 y 2020, lo cual refleja un mecanismo oportuno y quizás mucho más eficiente debido a su frecuencia frente a la queja o la denuncia incoada por el titular de datos.

Además, la cifra de 135 multas impuestas por la SIC con ocasión de vulneración de PDP desde el 2018, necesariamente corresponde a un proceso sancionatorio llevado a cabo por la misma en la cual se contempló la multa como sanción por infringir el régimen normativo de PDP.

A su vez, la DIPDP señaló que entre otras ordenes administrativas iniciadas por la SIC en el último año se iniciaron en contra de las compañías Rappi S.A.S, Wikimujeres S.A.S y Cotech S.A., sin mencionar las investigaciones preliminares a la fecha contra Zoom y Tiktok. (DIPDP, 2020)

Por último, la DIPDP expuso que, durante la época de cuarentena nacional en la cual se vio un incremento del uso de medios digitales y electrónicos debido a los decretos nacionales como el Decreto 990 del 09 de julio de 2020, que ordenó el aislamiento obligatorio, se implementaron herramientas "especializadas en supervisión basada en riesgos, bajo la premisa según la cual **el tratamiento de datos personales lleva implícito un riesgo**. Lo anterior en cumplimiento de los principios constitucionales de eficacia y eficiencia" (negrilla fuera del texto) (DIPDP, 2020) Si bien la SIC expresó emplear herramientas de supervisión *in situ* y *extra situ* que producen informes y monitoreos periódicos (DIPDP, 2020) Nuevamente se fomenta la actuación oficiosa de la SIC a través de la DPDP, mediante la ejecución del principio accountability.

Teniendo en cuenta los datos expuestos por la DIPDP se identifica que el mecanismo de quejas y denuncias no es frecuentado por los usuarios de entornos digital. En este aspecto, se fortalece aún más la paradoja de la privacidad a la que se ven envueltos los titulares de datos y usuarios de los entornos digitales. Esto es, entregar sus datos personales, autorizar su tratamiento, aunque ello implique un riesgo y posible vulneración de los mismos, debido a que es necesario, aceptar las políticas de datos que pactan las empresas, para poder acceder a los servicios que estas

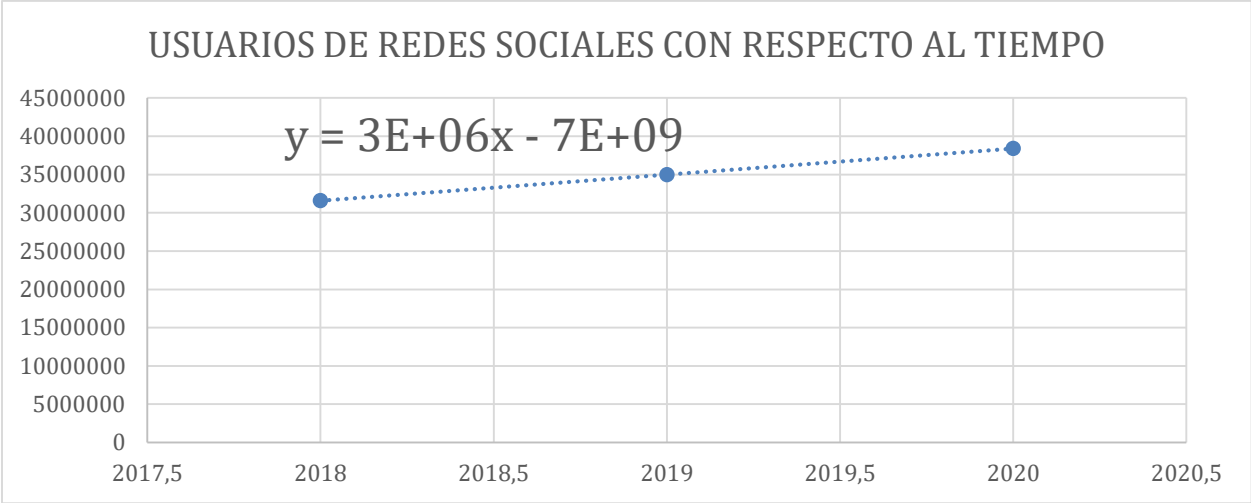
ofrecen. Lo anterior genera escenarios de perfilamiento de datos, filtración de información, vulneraciones al principio de libertad, transparencia, finalidad entre otros.

Para llevar al ejemplo un poco más el riesgo de vulneración a la PDP de los usuarios en el territorio colombiano se presentan las siguientes graficas relacionadas:

Figura 8. Número de consultas de usuarios ante la SIC con respecto al tiempo.


Nota*: Datos tomados a partir de la publicación en la red social Instagram desde la cuenta de la SIC el 09 de agosto de 2020. En el cual señaló registrar 23.252 solicitudes ciudadanas desde el año 2018 hasta el año de publicación. Por Yahaira Arévalo Aragón, 2020

Figura 9. Usuarios de redes sociales con respecto al tiempo.




Nota*: Datos tomados a partir de las cifras publicadas en la página web *Branch* sobre Estadísticas de la situación digital de Colombia en el 2019 y 2020. Adaptado de (Rosgaby, 2020), Por Yahaira Arévalo Aragón, 2020

Como se expone en las gráficas precedentes, el porcentaje de usuarios de redes sociales en Colombia aumentó en un 11.5% del año 2019 al 2020, a partir de allí se proyecta el incremento de los mismos con respecto al tiempo, el cual arroja un comportamiento directamente proporcional.

Actualmente Colombia es el segundo país a nivel mundial, a enero de 2020, que pasa más tiempo en redes sociales. (Branch, 2020) Si se tiene en cuenta estas cifras con respecto a la cantidad de solicitudes presentadas ante la SIC con ocasión de la PDP, se identifica un comportamiento proporcional, es decir que, si aumenta el número de usuarios con respecto al tiempo lo mismo sucederá en relación del número de solicitudes dirigidas a la SIC. Es relevante puntuar que las denuncias y quejas no son datos incluidos dentro del grafico por sus menores cifras, de hecho, volviendo a las denuncias, si el total de usuarios en redes sociales es de 38.5 millones y hay 23.252 solicitudes, significa que menos del 0.67% utiliza este mecanismo administrativo.

La SIC, como autoridad legal para garantizar y procurar por la protección de los datos personales, debe fortalecer sus funciones. La cantidad de sanciones, como multas, realizadas a quienes realizan TDP deja una cifra preocupante sobre el panorama social respecto a la importancia de ejercer los derechos que le asisten para la protección sus datos personales; implica la necesidad de poner mayor atención en las prácticas de TDP, sobre todo, en las políticas de tratamiento de datos y los términos de las mismas, identificar si estas son abusivas o si por el contrario se ajustan a la normativa colombiana, y a su vez, si aseguran un nivel adecuado de protección de datos personales según los estándares internacionales.

## Conclusiones

El ordenamiento jurídico colombiano consagra la protección de datos y habeas data como un derecho fundamental descrito en el artículo 15 constitucional. Inicialmente, el habeas data se entendía únicamente por la taxatividad del articulo mencionado, no contemplaba las facultades atribuidas actualmente al TD para autorizar cada uno de los TDP que se realicen sobre sus datos personales e incluso suprimirlos, de las bases de datos, cuando lo considere.

La jurisprudencia nacional, especialmente la de la Corte Constitucional, se ha encargado de interpretar este artículo bajo los términos constitucionales, llegando a la conclusión que el TD tiene derecho, entre otros, a su determinación informática, y que esta acompaña al TD incluso en el entorno digital. La determinación informática faculta al TD a ejercer control sobre la información usada, recolectada y almacenada en las diferentes bases de datos.

Por lo tanto, el TD puede en cada una de las etapas del TDP, ejercer el derecho a estar al tanto de cada una de las practicas realizadas durante el TDP. Lo anterior implica que, el tratamiento de datos personales es una práctica regulada desde la Constitución Política colombiana.

Anterior a las leyes estatutarias mencionadas a continuación, el ordenamiento jurídico colombiano se fundamentó en el derecho al habeas data del artículo 15, el derecho a la información del artículo 20 y el derecho a la libertad del artículo 28 constitucionales, y en las consideraciones jurisprudenciales de la Corte Constitucional.

En Colombia se identificó dos disposiciones fundamentales para la protección de datos personales, estas son la Ley Estatutaria 1266 del año 2008 y la Ley Estatutaria 1581 del año 2012. La primera obedece al campo del habeas data financiero, y la segunda regula el habeas data de manera genérica, por lo tanto, siempre se deberá observar esta ley y los principios allí contemplados para asegurar la protección de datos personales cuando el encargado o responsable de tratamiento de datos realice alguna practica como recolección, uso, almacenamiento o cualquiera que implique el tratamiento de dato personal de un titular de datos en el territorio nacional, cabe mencionar, que por territorio nacional se debe entender incluso las prácticas de TDP

que se realicen en domicilio fuera de Colombia, pero que para ello usen cookies o ficheros, como ha mencionado la SIC o la Corte Constitucional. Sin embargo, esta consideración debería ampliar a cualquier medio que permita el TDP, mediante la instalación o uso de un equipo tecnológico que use el titular de datos, y realice TDP.

A su vez, los Decretos 1733 del año 2013, 886 del año 2014 y el Decreto Único Reglamentario 1074 del año 2015, que compiló entre otras, todas las disposiciones en materia de protección de datos; fomentan la búsqueda de un nivel de protección de datos alto. La implementación de la responsabilidad demostrada o accountability, por ejemplo, era una disposición necesaria para proteger los datos personales, esta figura tiene origen en el marco supranacional.

En cuanto al estado actual de protección de datos personales en Colombia, el camino para alcanzar un nivel adecuado de protección de datos en los términos de los estándares internacionales es largo. Si bien, Colombia adoptó diferentes disposiciones en materia de protección de datos como lo es los Estándares de Protección de Datos de la RIPD, la cual contempla disposiciones del mismo sentido que las Directrices de la OCDE, los Principios de la OEA e incluso la Resolución 45/95, al adoptar figuras como la responsabilidad demostrada o accountability, el principio de trasparencia, el fortalecimiento y des limitación del flujo trasfronterizo de datos cuando se cuente con un nivel adecuado de protección de datos personales, Colombia necesita más precisión en sus normativas de protección de datos personales, la Ley 1581 de 2012, por ejemplo, ofrece un campo muy genérico, lo ideal es remitirse a las guías realizadas por la SIC en la materia con base en disposiciones internacionales para entender la protección de datos personales.

Respecto a los mecanismos dispuestos en la normativa colombiana para la protección de datos personales, se encuentran, como mecanismos administrativos la queja, petición o consulta, promovida por el titular de datos, e incluso la ley faculta al causahabiente, para la protección de sus datos personales, contra el encargado o responsable del TDP. En cuanto a la denuncia, es necesario agotar el mecanismo administrativo para acceder a este mecanismo judicial, en el cual conoce en principio la SIC, facultada para sancionar. Además, la ley permite que estos mecanismos se dirijan en contra del encarga o del responsable del TDP, en el caso en que recaigan las funciones del TDP en uno u otro. Sin embargo, los usuarios de entornos digitales no frecuentan estos

mecanismos lo que permite considerar una ausencia de interés en la PDP o bien, un desconocimiento sobre la existencia del mismo.

De igual forma, se puede acceder a la acción de tutela, como mecanismo judicial subsidiario de protección de datos o bien, iniciar un proceso en el ámbito civil bajo los postulados del artículo 16 de la ley 1266, o bajo un proceso de responsabilidad civil contractual de habeas data. Es importante precisar que, los mecanismos judiciales diferentes de la tutela son de una aplicación principalmente en cuanto a la materia del habeas data financiero, es decir de la Ley 1266 del 2008.

Como último mecanismo se estudió el principio de responsabilidad demostrada o accountability, el cual busca una protección preventiva, proactiva y constante encargada a quienes realizan TDP. Accountability es un principio supranacional que es consagrado y practicado en el ordenamiento jurídico colombiano, lo que permite que se acojan su naturaleza proactiva y permita alcanzar un nivel adecuado de protección de datos personales. La SIC es la encargada, a través de la Delegatura para la Protección de Datos Personales de ejercer en todo momento el control y vigilancia sobre las empresas públicas o privadas que realizan TDP. Así que, corresponde a la SIC realizar las actividades de vigilancia pertinentes para dar cumplimiento con la responsabilidad demostrada.

Lo trascendental del principio accountability es que no se basa en un simple reglamento o política interna de la empresa que realiza TDP, por el contrario, es un control permanente de seguridad y protección de datos personales. Sin embargo, es preciso señalar que este principio por sí solo no representa una salida rápida para alcanzar un nivel adecuado para la protección de datos personales. Es necesaria la implementación de políticas internas como la privacidad por defecto en especial en el uso de IA o algoritmos que realicen TDP, permitiendo minimizar las vulneraciones a la protección de habeas data como filtraciones, usos no autorizados, perdida de datos entre otros. La SIC ha hecho un claro uso del principio accountability y ha iniciado de oficio investigaciones, como es el caso de las compañías Facebook, Zoom o TikTok, en búsqueda de procurar por el cumplimiento de la normativa colombiana en materia de PDP.

El desafío que representan los constantes desarrollos en el entorno digital para el ordenamiento colombiano es alto. El Estado colombiano debe prepararse mediante la implementación de normas puntuales, eficientes, que atiendan las realidades sociales actuales. Es preciso fortalecer la implementación del principio de trasparencia y principio de proporcionalidad al interior de las empresas que realizan TDP. El principio de proporcionalidad no se encuentra consagrado en la ley nacional, como la ley 1581 o el decreto 886, y aunque es abordado en los Estándares de la RIPD del cual es parte Colombia, es necesario que las normas reglamenten puntualmente el uso de los TDP, frente a la autorización del TDP y las cláusulas que señalan las empresas para que el titular de datos y usuario del entorno digital pueda acceder a los servicios o productos que ofrezca la misma. El mayor riesgo que presenta la PDP es el profiling como resultado de la inobservancia de principios como la finalidad, transparencia o proporcionalidad en la PDP. Además, profiling pretende ser una práctica común en el entorno digital por lo que resulta pertinente su regulación a tiempo.

Las autoridades colombianas y la ley, debe estar dirigida a evitar, por ejemplo, cláusulas abusivas como las señaladas en la política de datos de Facebook, al determinar TDP demasiado amplios, poco proporcionales, con finalidades de TDP extensas, que les permite casi que realizar TDP de manera ilimitada como el profiling. La ley colombiana debe abordar esta problemática a partir de la fomentación del principio de proporcionalidad, el principio de la finalidad del uso o TDP y el principio de accountability.

Del mismo modo, el papel funcional de la Delegatura para la Protección de Datos Personales, es fundamental para promover y garantizar la protección de los mismos. Si bien, los resultados de la respuesta emitida por la SIC a través de la Dirección de Investigación para la Protección de Datos, mostró una participación poco activa de los titulares de datos frente a la presentación de quejas, peticiones o denuncias por motivos de protección de datos, es oportuno remitirse a la paradoja de la privacidad, saber que se pueden vulnerar sus derechos, pero de igual forma correr el riesgo. La SIC, como autoridad, debe procurar por evitar la vulneración de habeas data mediante la vigilancia constante y eficiente a las empresas que realizan TDP.

## Referencias Bibliográficas

Agüero, I. (2019). La Protección de Datos Frente al Alto Grado de Libertad de la GAFA (Google, Apple, Facebook y Amazon): La solución que importa la nueva regulación europea frente a la regulación norteamericana. Revista de Derecho Universidad San Sebastián, 20–28. https://doctrina.vlex.cl/vid/proteccion-datos-frente-alto-783556253

Angarita, N. R. (2011). Documento Gecti Nro. 11 Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del habeas data y la protección de los datos personales. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 6, 3–8. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Doc-GECTI-11-propuesta-mejora-proyecto-de-ley1.pdf

Asamblea General de la Organización de Estados Americanos (OEA). (2011). Principios y Recomendaciones Preliminares Sobre la Protección de Datos CP/CAJP-2921/10. https://www.oas.org/dil/esp/CP-CAJP-2921-10_esp.pdf

Asamblea General de las Naciones Unidas. (14 diciembre de 1990). Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales. Resoluciones aprobadas por la asamblea general durante el 45° período de sesiones. https://www.un.org/es/documents/ag/res/45/list45.htm

Asamblea General de las Naciones Unidas. (1789). Declaración Americana de los Derechos y Deberes del Hombre. http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Asamblea General de las Naciones Unidas. (1948). La Declaración Universal de Derechos Humanos. https://www.un.org/es/universal-declaration-human-rights/

Asamblea General de las Naciones Unidas. (1979). Pacto Internacional de Derechos Civiles y Políticos. https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Bundesgerichtshofs. (23 junio 2020). Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook [El Tribunal Federal de Justicia confirma provisionalmente la acusación de abuso de una posición dominante por parte de Facebook]. https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html

Cambridge Dictionary. (2020). Significado de profiling en inglés. https://dictionary.cambridge.org/es/diccionario/ingles/profiling

Casas Roma, J. Nin Guerrero, J. y Julbe López, F. (2019). Big data: análisis de datos en entornos masivos. Editorial UOC. https://elibro.net/es/ereader/usta/117744?page=128

Consejo de Europa. (2019). Manual de legislación europea en materia de protección de datos. Agencia de los Derechos Fundamentales de la Unión Europea. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

Constitución Política de Colombia [C.P.C] (1991) 36ª Ed. Legis

Corte Constitucional de Colombia, Sala Octava de Revisión de la Corte Constitucional. Sentencia T-260 (29 de marzo de 2012). [M.P. Humberto Antonio Sierra Porto]. https://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM#:~:text=T%2D260%2D12%20Corte%20Constitucional%20de%20Colombia&text=Los%20derechos%20fundamentales%20de%20los,nuestro%20Estado%20Social%20de%20Derecho.

Corte Constitucional de Colombia, Sala Plena de la Corte Constitucional. Sentencia C-1011. (16 de octubre de 2008). [MP Jaime Córdoba Triviño] https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional de Colombia, Sala Plena de la Corte Constitucional. Sentencia C-748. (06 de octubre de 2011). [M.P. Jorge Ignacio Pretelt Chaljub] https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Constitucional de Colombia, Sala Primera de Revisión de la Corte Constitucional. Sentencia T-414. (16 de junio de 1992). [M.P. Ciro Angarita Baron] https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Corte Constitucional de Colombia, Sala Primera de Revisión de la Corte Constitucional. Sentencia T-634. (13 de septiembre de 2013). [M.P. María Victoria Calle Correa] https://www.corteconstitucional.gov.co/relatoria/2013/t-634-13.htm

Corte Constitucional de Colombia, Sala Primera de Revisión. Sentencia T-114. (03 de abril de 2018) [M.P. Carlos Bernal Pulido] https://www.corteconstitucional.gov.co/relatoria/2018/t-114-18.htm

Corte Constitucional de Colombia, Sala Séptima de Revisión de la Corte Constitucional. Sentencia T-729. (05 de septiembre de 2011). [M.P. Eduardo Montealegre Lynett] https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Suprema de Justicia de Colombia, Sala de Casación Civil. Sentencia SC3653-2019. (10 de septiembre de 2019). [M.P. Luis Armando Tolosa Villabona] https://cortesuprema.gov.co/corte/wp-content/uploads/2019/09/SC3653-2019.pdf

Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial 49523. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019935

Decreto 1377. (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012.. Diario Oficial 48.83. http://www.suin-juriscol.gov.co/viewDocument.asp?id=1276081

Decreto 4886 (23, diciembre, 2011). Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones. Diario Oficial 48294. http://www.secretariasenado.gov.co/senado/basedoc/decreto_4886_2011.html

Delon, V. M. (2019). La protección de datos personales mediante una garantía constitucional. México: Instituto de la Judicatura Federal. https://www.ijf.cjf.gob.mx/publicrecientes/2019/Datos%20Personales/DATOS%20PRESONALES%20COMPLETO.pdf

Dirección de Investigación de Protección de Datos Personales, (17 de julio de 2020). Respuesta a la petición realizada ante la Superintendencia de Industria y Comercio. Bogotá. DIPDP

El Tiempo. (2020). Trump anuncia que prohibirá a TikTok en EE. UU. https://www.eltiempo.com/noticias/tik-tok

Facebook. (2020). Política de Datos. https://es-es.facebook.com/privacy/explanation/

Fernández, Rosa. (2020). Statista. Evolución anual de los ingresos mundiales de Facebook desde 2010 hasta 2019. https://es.statista.com/estadisticas/525671/ingresos-mundiales-anuales-de-facebook/

GAL, Michel. & NIVA Elkin-Koren. (2017) Algorithmic Consumers. *Harvard Journal of Law and Technology*, Vol. 30, 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2876201

Galvis Cano, L. (2018). El Panóptico digital de la protección de datos personales en Colombia. *Revista Temas*, 3(12), 125–140. https://doi.org/10.15332/rt.v0i12.2038

González Guerrero, L. D. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. Estudios Socio-Jurídicos, 21(1), 209-244. Doi: http://dx.doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941

González Martín, N. & Albornoz, M. M. (diciembre, 2014). Comercio electrónico, Online Dispute Resolution y desarrollo. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 12. Universidad de los Andes (Colombia). http://dx.doi.org/10.15425/redecom.12.2014.12

Google. (26 de julio 2020). Acerca de los ID de publicidad para móviles. https://support.google.com/admanager/answer/6274238?hl=es

Helberger, N. (6 de febrero de 2016). Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717

Hernández, J., Ramírez, M., Ferri, C. (2004). Introducción a la minería de datos. Pearson Educación. http://ebooks7-24.com.crai-ustadigital.usantotomas.edu.co/?il=3281

Katherine-Chen, Y., & Ryan-Wen, C. (2019). Taiwanese university students' smartphone use and the privacy paradox. [Uso del teléfono inteligente en universitarios taiwaneses y la paradoja de la privacidad]. Comunicar, 60, 61-70. https://doi.org/10.3916/C60-2019-06

La República. (1 abril 2020). Apps de domicilios y salud registran aumento de descargas durante la cuarentena. https://www.larepublica.co/empresas/apps-de-domicilios-y-salud-registran-aumento-de-descargas-durante-la-cuarentena-2986689

La Vanguardia. (2017) El 75% de las empresas que usaron inteligencia artificial elevaron un 10% sus ingresos, según Capgemini. https://www.lavanguardia.com/vida/20170907/431110394802/economia--el-75-de-las-empresas-que-usaron-inteligencia-artificial-elevaron-un-10-sus-ingresos-segun-capgemini.html

Laudon, K. & Guercio, C. (2014). E-commerce 2013. (9a. ed.) Pearson Educación. http://ebooks7-24.com.crai-ustadigital.usantotomas.edu.co/?il=3298

Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros

países y se dictan otras disposiciones. Diario Oficial 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Ley Estatutaria 1581. (17. Octubre, 2012). de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Martínez, Devia, A. (2019) La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial* n.° 27, Universidad Externado de Colombia, enero-junio 2019, pp. 5-23. doi: https://doi.org/10.18601/16571959.n27.01

Ministerio de Tecnologías de la Información y Comunicaciones (Min Tic). (Actualizado el: jueves, 28 de mayo de 2020). El 1,8% de las empresas en Colombia utiliza Inteligencia Artificial. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los Medios/79933:El-1-8-de-las-empresas-en-Colombia-utiliza-Inteligencia-Artificial

Nougrères, A. B. (2007). El Sistema Legal Uruguayo De Protección De Datos Personales. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 3, 1–30. https://dialnet.unirioja.es/descarga/articulo/7510287.pdf

Organización de Cooperación y Desarrollo Económico. (1980). Directrices Relativas a la Protección de datos personales y Flujos Trasfronterizos de Datos Personales. http://www.oas.org/es/sla/ddi/proteccion_datos_personales_otros_documentos.asp#Naciones_Unidas_(ONU)

Organización de Cooperación y Desarrollo Económico. (2002). Resumen, Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. http://www.oecd.org/sti/ieconomy/15590267.pdf

Organización de Cooperación y Desarrollo Económico. (7-9 octubre de 1998). Declaración ministerial relativa a la protección de la intimidad en las redes globales. http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf

Organización de Cooperación y Desarrollo Económico. (9 diciembre de 1999). Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico. http://www.oecd.org/sti/consumer/34023784.pdf

Organización de los Estados Americanos. (1969). Convención Americana Sobre Derechos Humanos (Pacto De San José). http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Parlamento del Uruguay. (1967). Constitución de la República. https://parlamento.gub.uy/documentosyleyes/constitucion

Pew Research Center y Hitlin, P. & Rainie, L. (2019). “Facebook Algorithms and Personal Data” https://www.academia.edu/download/59250358/Facebook_algorithms_report20190514-34280-jrzed3.pdf

Point Zero Production Inc. (2020). Conexiones. [episodio 1 serie documental] Netflix

Polo Roca, Andoni. Sociedad de la Información, Sociedad Digital, Sociedad de Control. Inguruak, [S.l.], n. 68, jun. 2020. ISSN 0214-7912. <http://www.inguruak.eus/index.php/inguruak/article/view/177>.

Rappi S.A.S. (2020). Política de Tratamiento de Datos Personales. https://legal.rappi.com/colombia/politica-de-proteccion-y-tratamiento-de-datos-personales-rappi-s-a-s/

Real Academia Española (RAE). (2020a). Definición de perfilado - Diccionario del español jurídico https://dle.rae.es/perfilado

Real Academia Española (RAE). (2020b). Definición de perfilar - Diccionario del español jurídico https://dle.rae.es/perfilar?m=form

Real Academia Española (RAE). (2020c). Definición de red social - Diccionario del español jurídico https://dej.rae.es/lema/red-social

Red Iberoamericana de Protección de Datos Personales (RIPD). (2017). Estándares de protección de datos personales para los estados iberoamericano https://www.redipd.org/sites/default/files/inlinefiles/Estandares_Esp_Con_logo_RIPD.pdf

Red Iberoamericana de Protección de Datos Personales (RIPD). (2019). Historia de la Red Iberoamericana de Protección de Datos (RIPD) https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd

Remolina-Angarita, N. (2010). ¿Tiene Colombia Un Nivel Adecuado De Protección De Datos Personales a La Luz Del Estándar Europeo? *International Law*, 17, 489–523. https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847/11142

Remolina-Angarita, N. (2015). Recolección internacional de datos personales: un reto del mundo postmoderno. Boletín oficial del estado. https://gecti.uniandes.edu.co/images/pdf/1-

Remolina-2015-recoleccion-internacional-de-datos-personales-reto-del-mundo-post-internet.pdf

Resolución 12192 (01 de abril de 2020). Sobre de protección de datos personales en la Red social Facebook en Colombia. Superintendencia de Industria y Comercio [SIC]. https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%2001IV2020%20SIC%20Facebook%20Inc.pdf

Resolución 24913. (29 de mayo de 2020). Por la cual se resuelve un recurso de apelación sobre de protección de datos personales. Superintendencia de Industria y Comercio [SIC]. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/R%2024913%20-%2029-05-2020%20Banco%20de%20Bogot%C3%A1.pdf

Resolución 30412. (23 de junio de 2020). Por la cual se resuelve un recurso de apelación sobre de protección de datos personales. Superintendencia de Industria y Comercio [SIC]. https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Res%2030412%20-%2023-06-2020%20-%20Fotografo%20Hotel%20Diez.pdf

Resolución 76434. (05 de diciembre de 2012). Por la cual se deroga el contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado Título. Superintendencia de Industria y Comercio [SIC]. https://www.sic.gov.co/sites/default/files/normatividad/Resolucion_76434_2012.pdf

Riquelme Santos, J.C., Ruíz, R. y Gilbert, K. (2006). Minería de Datos: Conceptos y Tendencias. Inteligencia Artificial: *Revista Iberoamericana de Inteligencia Artificial*, 10 (29), 11-18. https://idus.us.es/bitstream/handle/11441/43290/Miner%c3%ada%20de%20datos.pdf?sequence=1&isAllowed=y

Rosgaby, K. (17, abril, 2020). Estadísticas de la situación digital de Colombia en el 2019 y 2020. Branch Group. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/

San Juan Rodríguez, N. (2019). Inteligencia Artificial Y Propiedad Intelectual. Actualidad Jurídica (1578-956X), 52, 82–94. https://web-b-ebscohost-com.crai-ustadigital.usantotomas.edu.co/ehost/detail/detail?vid=4&sid=1144164e-8a5a-4a1f-ae1f-

31d4c8989cc5%40pdc-v-sessmgr04&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=142290629&db=a9h

Schiavi, P. (2017). El Derecho Al Olvido y a la Protección de Datos Personales en Uruguay. Revista de Derecho (15105172), 16(31), 55–74. http://revistaderecho.um.edu.uy/wp-content/uploads/2017/09/SCHIAVI-Pablo-El-derecho-al-olvido-y-a-la-proteccion-de-datos-personales-en-Uruguay.pdf

Superintendencia de Industria y Comercio (SIC). (2015). Guía para la Implementación de Responsabilidad Demostrada (Accountability). https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Superintendencia de Industria y Comercio (SIC). (2018). Datos tomados de la cuenta oficial de la red social Instagram de la SIC. https://www.instagram.com/p/CDl8WbpJA16/

Superintendencia de Industria y Comercio (SIC). (2019) Guía para la implementación del principio de responsabilidad demostrada. En las transferencias internacionales de datos personales. https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

Superintendencia de Industria y Comercio (SIC). (2019) Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

Superintendencia de Industria y Comercio (SIC). (2019). Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20(2019)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf

Superintendencia de Industria y Comercio (SIC). (2020) Superindustria investigará a plataforma de videoconferencias Zoom para establecer si protege adecuadamente datos de los colombianos. https://www.sic.gov.co/slider/superindustria-investigar%C3%A1-plataforma-de-videoconferencias-zoom-para-establecer-si-protege-adecuadamente-datos-de-los-colombianos

Superintendencia de Industria y Comercio (SIC). (2020). Normatividad. https://www.sic.gov.co/repositorio-de-normatividad?field_tipo_de_norma_value=3

Superintendencia de Industria y Comercio. (2020a). BIG DATA le cuenta sobre el valor de sus datos personales. https://www.sic.gov.co/slider/big-data-le-cuenta-sobre-el-valor-de-sus-datos-personales

Superintendencia de Industria y Comercio (SIC). (2020b). Superintendencia de Industria y Comercio. Delegatura de Protección de Datos Personales ¿Qué es? https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia de Industria y Comercio (SIC). (2020c). Sobre la protección de datos personales. https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia de Industria y Comercio (SIC). (2020, 9 de agosto) La Delegatura para la Protección de Datos Personales garantiza que en el tratamiento de tus datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley. #CompromisoSIC. [Fotografía] https://www.instagram.com/p/CDl8WbpJA16/

Suprema Corte de Justicia de la Nación. México. Semanario Judicial de la Federación. (21 febrero 2020). Sentencia de constitucionalidad 29318. https://sjf.scjn.gob.mx/SJFSem/Paginas/ResultadosV2.aspx?Clase=SemanarioEjecutoriaBL&Expresion=proteccion%20de%20datos&Dominio=Tema,Texto&SemanaId=202008&Orden=3&Tablero=-100

Terceiro, J. B. (1996). Sociedad digital. Del homo sapiens al homo digitalis. Madrid. Editorial Alianza

Tribunal de lo Contencioso Administrativo. Uruguay. (16 de julio de 2013) Sentencia Nº 350 de 2013 https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/sentencia-del-tribunal-contencioso-administrativo-350-16-julio-2013

Unión Europea. Reglamento General de Protección de Datos. (2016). https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Vega Freddy, (2020) *Forbes Colombia*. 2020: el año de la Inteligencia Artificial. https://forbes.co/2020/01/31/red-forbes/2020-el-ano-de-la-inteligencia-artificial/

# Anexo

## Anexo 1. Derecho de petición

Industria y Comercio
SUPERINTENDENCIA

Bogotá D.C.

Señora
**YAHAIRA AREVALO ARAGÓN**
yahairaarego@gmail.com

Asunto: Radicación: 20-133430- - 3-0
Trámite: 384
Evento: 328
Actuación: 440
Folios: 4

En atención a las comunicaciones radicadas por usted ante esta Dirección bajo el número **20-133430 y 20-136951**, es necesario informarle que, en acatamiento de las disposiciones proferidas por la Presidencia de la República y la Superintendencia de Industria y Comercio, relacionadas con la Emergencia Sanitaria - Ambiental declarada ante la pandemia del COVID -19, a fin de salvaguardar sus garantías como Titular del derecho fundamental de *habeas data*, esta Delegatura procede a resolver su petición, teniendo en cuenta que el Decreto 491 de 2020 del 28 de marzo de 2020, en su artículo 5 amplia los términos señalados en el artículo 14 de la Ley 1537 de 2011 para responder las peticiones que se encuentren en curso o que se radiquen durante la vigencia de la emergencia sanitaria, esta Dirección se encuentra en tiempo para resolver su petición, y lo hace en los siguientes términos:

**A. ¿Cuál es el marco normativo (leyes, decretos y resoluciones) de protección y regulación de datos personales en Colombia?**

Al respecto, esta Superintendencia se permite señalar las normas actuales (derechos constitucionales, leyes, decretos, resoluciones, que regulan o inciden en el tema de protección de datos personales en Colombia:

1. Constitución Política de Colombia: Artículo 15.

2. Frente al tratamiento de datos personales de carácter financiero, crediticio y comercial y proveniente de terceros países, es regulado por la Ley 1266 de 2008 y sus decretos reglamentarios (Decreto 1727 de 2009 – Decreto 2952 de 2010) compilados en los capítulos 27 y 28 del Decreto Único 1074 de 2015.

Industria y Comercio
SUPERINTENDENCIA

Teniendo en cuenta que la ley 1266 de 2008 es una Ley Estatutaria, es referencia la Sentencia C-1011 de 2008, por medio de la cual se declaró la exequibilidad de la misma.

En concordancia, el Titulo V de la Circular Única de la Superintendencia de Industria y Comercio, Resolución 76434 de 2012, en su Capítulo Primero, regula el ejercicio del derecho de habeas data de información financiera, crediticia y comercial y la proveniente de terceros países.

3. Por su parte, respecto a las disposiciones generales para la protección de datos personales, la Ley 1581 de 2012 Capítulo 25 y 26 del Decreto Único 1074 de 205, que compiló los Decretos 1377 de 2013 y el Decreto 886 de 2014.

   Teniendo en cuenta que la ley 1266 de 2008 es una Ley Estatutaria, es referencia la Sentencia C-748 de 2011, por medio de la cual se declaró la exequibilidad de la misma.

   Así mismo, el Titulo V de la Circular Única de la Superintendencia de Industria y Comercio, en su Capítulo Segundo, regula temas relacionados con el registro Nacional de Bases de datos, y en su Capítulo Tercero, regula lo relacionado con las Transferencias Internacionales.

**B. ¿Cuál es el marco normativo (leyes, decretos y resoluciones) de protección y regulación de datos personales en Colombia frente a redes sociales, e-commerce y portales de contacto?**

Teniendo en cuenta que, el artículo 2 de la Ley 1581 de 2012, estableció el ámbito de aplicación, según el cual *"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada".*

Así mismo, contempló 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 territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".*

En consecuencia, cuando exista tratamiento de datos personales en bases de datos o archivos por parte de personas naturales o jurídicas, de derecho público o privado, tanto en el territorio nacional como cuando el Responsable o Encargado del tratamiento que no establecido en el territorio le sea aplicable la Ley Colombiana, le será aplicable la Ley 1581 de 2012.

Industria y Comercio
SUPERINTENDENCIA

De manera complementaria, se le informar que esta Superintendencia ha elaborado Guías para la aplicación de la Ley 1581 de 2012, en diferentes ámbitos, a las cuales puede acceder a través del enlace de la publicaciones: https://www.sic.gov.co/centro-de-publicaciones?field_tema_general_tid=5&field_anos_p_value=All, En dicho enlace Ud. puede acceder a las siguientes guías:

- Guía para el tratamiento de datos personales para el sector de la educación pública y privada (2015).
- Guía de Protección de los Datos Personales en los Servicios de Computación en la Nube (Cloud Computing). (2015).
- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability). (2016)
- Guía para solicitar la declaración de conformidad sobre las transferencias internacionales de datos personales. (2016).
- Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. (2019).
- Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial. (2019).
- Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales. (2019)
- Guía sobre el tratamiento de datos personales para fines de comercio electrónico (2019).

**C. ¿Por qué motivo se han generado las actuaciones en cuanto a protección de datos personales en cuanto a entornos de redes sociales, e-commerce y portales de contacto?**

Al respecto nos permitimos informar que los motivos por los cuales se han generado actuaciones administrativas en materia de protección de datos personales en cuanto a redes sociales, e-commerce y portales de contacto, son las siguientes:

1. Infracción al deber y principio de seguridad, confidencialidad e integridad de la información, es decir, insuficientes e inadecuadas medidas técnicas, humanas y administrativas para garantizar seguridad a los datos personales con el fin de evitar adulteraciones, pérdidas, consultas, usos o accesos no autorizados o fraudulentos.

2. Infracción al deber de obtener la autorización previa, expresa e informada del titular e informar lo que ordena el artículo 12 de la Ley 1581 de 2012.

Industria y Comercio
SUPERINTENDENCIA

3. Infracción al deber de adoptar, implementar y desarrollar políticas de seguridad de la información y procedimientos para la recolección, almacenamiento, uso, circulación, supresión y disposición final de la información.

4. Infracción al deber de adoptar, publicar en sitio web, implementar y desarrollar una Política de Tratamiento de Datos Personales.

5. Infracción al deber de adoptar, publicar e implementar un Manual Interno de Políticas y Procedimientos para la atención de consultas y reclamos de los titulares.

6. Infracción al deber de conservar prueba de la autorización previa, expresa e informada otorgada por el titular.

7. Infracción al deber de garantizar al titular en todo tiempo el pleno y efectivo ejercicio del derecho de habeas data.

**D. ¿Cuántas denuncias, quejas o reclamos han sido recibidas por la SIC en el periodo 2018 a la actualidad en cuanto a vulneraciones al derecho de protección de datos personales en el entorno digital?**

- Total de quejas: Treinta y cuatro (34)
- Comercio al por menor realizado por internet: Dos (2)
- Redes sociales: Una (1)
- Portales web: Veintinueve (29)
- Apps transporte: Dos (2)

**E. ¿Cuántas sanciones se presentan anualmente (2018, 2019, 2020) por vulneración de datos personales en el entorno digital?**

- 2018: Dos (2) por literal a y d del artículo 17 de la Ley 1581 de 2012.
- 2019: Dos (2) por literal b y c del artículo 17 de la Ley 1581 de 2012.
- 2020: A la fecha no hay sanciones frente a entornos digitales.

**F. ¿Se presenta mayor vulneración de protección de datos personales en alguna de las redes usadas normalmente por los usuarios?**

A la fecha no existen sanciones contra redes sociales, sin embargo sí se ha impartido una orden en contra de la red social Facebook, la cual puede ser consultada en el link

Industria y Comercio
SUPERINTENDENCIA

https://www.sic.gov.co/sanciones-proteccion-datos-personales-2019, así como todas las decisiones sancionatorias pueden ser consultadas en https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas.

**G. ¿Tienen las plataformas E-commerce y redes sociales regulación actualmente en Colombia? ¿Cuál es este marco normativo especializado?**

Al respecto, le reiteramos lo indicando en el literal B del cuestionario, según el cual, en materia de protección de datos, cuando exista tratamiento de datos personales en bases de datos o archivos por parte de personas naturales o jurídicas, de derecho público o privado, tanto en el territorio nacional como cuando el Responsable o Encargado del tratamiento que no establecido en el territorio le sea aplicable la Ley Colombiana, le será aplicable la Ley 1581 de 2012.

**H. ¿Qué regulación tienen las plataformas E-commerce y redes que no cuentan con domicilio en el país, pero que prestan sus servicios a través de internet en Colombia?**

Al respecto, le reiteramos lo indicando en el literal B del cuestionario, según el cual, en materia de protección de datos, cuando exista tratamiento de datos personales en bases de datos o archivos por parte de personas naturales o jurídicas, de derecho público o privado, tanto en el territorio nacional como cuando el Responsable o Encargado del tratamiento que no establecido en el territorio le sea aplicable la Ley Colombiana, le será aplicable la Ley 1581 de 2012.

**I. ¿Se ha presentado incremento en las denuncias realizadas por los usuarios de internet en atención a vulneración de protección de datos personales en los últimos meses del 2020?**

Las denuncias y/o quejas recibidas por usuarios de internet en el periodo 01/01/2019 al 31/05/2019 comparada con el mismo período 01/01/2020 al 31/05/2020 es el siguiente:

Total de quejas frente a entornos digitales período 01/01 al 31/05 de 2019 y 2020: 25

- Quejas 2019: 16 correspondiente al 64%
- Quejas 2020: 09 correspondiente al 36%

**J. ¿Ejerce la SIC control y vigilancia sobre las diferentes plataformas E-commerce y redes que prestan servicios en el país? ¿Cuáles son las actuaciones**

Industria y Comercio
SUPERINTENDENCIA

**administrativas realizadas en el último año para llevar a cabo este control y vigilancia?**

La Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales ejerce control y vigilancia, entre otros, a plataformas de e-commerce y redes sociales, facultad administrativa que ha ejercido de acuerdo con el artículo 21 de la Ley 1581 de 2012 de oficio o con ocasión de quejas presentadas por ciudadanos.

Pruebas de dicho control y vigilancia realizado en el último año sobre éstas plataformas de e-commerce y redes sociales son:

1. Las ordenes administrativas impartidas en contra de compañías como Facebook y Uber.

2. Las sanciones pecuniarias impuestas en contra de compañías como Rappi S.A.S., Asegúrate Facil Ltda., Wikimujeres S.A.S. y Cotech S.A.;

3. Las investigaciones preliminares abiertas en contra de Zoom y de Tiktok.

**K. ¿Cuál es el marco de contingencia empleado por la SIC, en atención al incremento del uso de internet y el mayor flujo de datos personales en los entornos digitales en los últimos meses, para asegurar la protección de los datos personales de los usuarios?**

La Superintendencia de Industria y Comercio, en cumplimiento de las funciones establecidas en el artículo 21 de la Ley 1581 de 2012[1] y como máxima autoridad de vigilancia y control en

[1] **ARTÍCULO 21. FUNCIONES.** La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:
a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;
b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;
c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;
d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;
e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;
f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

Industria y Comercio
SUPERINTENDENCIA

materia de protección de datos personales ha implementado un conjunto de herramienta especializadas en supervisión basada en riesgos, bajo la premisa según la cual el tratamiento de datos personales lleva implícito un riesgo. Lo anterior en cumplimiento de los principios constitucionales de eficacia y eficiencia. Se debe aclara que las herramientas utilizadas por la Delegatura para la Protección de Datos Personales son aplicables no sólo en los entornes digitales o virtuales sino también en los entonos físicos.

Adicionalmente debemos señalar que, junto con las herramientas mencionada adelantamos procedimientos de supervisión *in situ* (en el propio lugar) realizando visitas administrativas y de supervisión *extra situ* ( fuera de su lugar) generando informes periódicos de monitoreo y priorización que nos permite efectuar requerimientos posteriores a los sujetos obligados

Finalmente le informamos que, conforme al Decreto 990 del 09 de julio de 2020, proferido por la Presidencia de la República, por medio del cual se impartieron instrucciones en virtud de la emergencia sanitaria por la pandemia del Coronavirus COVID -19 y se ordenó el aislamiento preventivo obligatorio de todas las personas en Colombia y con ello la limitación total a la libre circulación de los habitantes del país, esta comunicación se envía a su correo electrónico; lo anterior, con la finalidad de atender en tiempo las peticiones radicadas ante esta Superintendencia.

En los anteriores términos damos respuesta a su comunicación y quedamos atentos a resolver cualquier inquietud sobreviniente.

Atentamente,

CARLOS ENRIQUE SALAZAR MUÑOZ
Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUÑOZ
Fecha: 2020.07.17 17:44:53 -05'00'

**CARLOS ENRIQUE SALAZAR MUÑOZ**
**DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES**

Elaboró: Nicolás Rojas
Revisó: Claudia B García / Aída Hurtado
Aprobó: Carlos Enrique Salazar Muñoz

---

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;
h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;
i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;
j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes;
k) Las demás que le sean asignadas por ley.