Habeas data y contratos electrónicos[1]

Habeas data and electronic contracts

Carlos Andrés Hernández Ávila[1]
Sara Ximena Pinzón Restrepo[2]

DOI: https://doi.org/10.18041/0124-0013/nuevaepoca.61.2024.12170

Resumen

El presente trabajo pretende realizar un análisis sobre la normatividad colombiana del derecho al habeas data, frente a los contratos electrónicos, en especial el de Facebook, para así constatar mediante la normatividad, la relación contractual y los estudios de caso, en que aspectos si es que los hay, pueden evidenciarse vulneraciones y que medidas la persona tiene para proteger su derecho fundamental al Habeas Data.

Palabras claves: Habeas data, información personal, información privada, Facebook, contratos electrónicos, condiciones contractuales.

Abstract

This paper aims to carry out an analysis on the Colombian normativity of the right to habeas data, compared to electronic contracts, especially that of Facebook, in order to verify through the normativity, the contractual relationship and the case studies, in which aspects, if any, violations can be evidenced and what measures the person has to protect his fundamental right to Habeas Data.

Key words: Habeas data, personal information, private information, Facebook, electronic contracts, contractual conditions.

Cómo citar este artículo: Hernández, C. A. y Pinzón, S. X. (2023). Habeas data y contratos electrónicos. Revista Nueva Época, (61), 59-84.

[1] La presente investigación ha sido elaborada al interior del Semillero de Derecho Privado y Económico de la Universidad Libre de Colombia, adscrito al Grupo de Investigación en Derecho Privado y del proceso de la Facultad de derecho -Sede Bogotá-.

[2] Estudiante de quinto año del programa de derecho de la Universidad Libre de Colombia. Sede Bogotá. Correo electrónico: carlosa-hernandeza@unilibre.edu.co Miembro del Semillero de Derecho Privado y Económico dirigido por el Dr. Jenner Alonso Tobar.

[3] Estudiante de quinto año del programa de derecho de la Universidad Libre de Colombia. Sede Bogotá. Correo electrónico: sarax-pinzonr@unilibre.edu.co. Miembro del Semillero de Derecho Privado y Económico dirigido por el Dr. Jenner Alonso Tobar.

Introducción

La evolución constante de la tecnología ha provocado un cambio en las dinámicas sociales, pues es muy poco probable que algún individuo no se encuentre afectado por el exponencial crecimiento del mundo tecnológico. Es así como hemos pasado de enviar cartas a simplemente enviar un mensaje a través de WhatsApp, de imprimir fotos a colgarlas en un Post en Instagram, de contar chistes en la calle a pasar horas viendo memes en Facebook, de buscar inspiración en el mundo externo a buscar ideas en Pinterest, de buscar información en las bibliotecas a buscarlas en Chrome, de comprar vinilos o Cd´s a utilizar Youtube o Spotify; todo esto gracias a un gran grado de eficiencia en el desarrollo de aplicaciones que buscan hacer más somera la vida.

Las redes sociales llegaron a finales del siglo pasado, y han evolucionado tanto a partir de ese momento, a tal punto que no es un tema novedoso sino algo habitual para este punto de la historia.

Facebook es una de estas redes sociales que se usan de manera constante y habitual en todo el mundo, incluyendo a Colombia, su empresa META, es dueña directa de otras redes sociales como lo son WhatsApp, Messenger, Instagram y Threads. Esta empresa es la competencia de la red social conocida anteriormente como Twitter, que hoy en día tiene el nombre de X. En cuanto a Facebook, al ser una red social que cuenta con demasiados usuarios, abarca una gran cantidad de sus datos personales, dentro de los cuales hay que saber qué tipo de datos y cómo es recopilada dicha información de los usuarios. Algunos de estos datos pueden ser de contenido delicado con el cual, si no se le hace un debido tratamiento y cuidado, puede perjudicar a la persona que los brindó.

Teniendo en cuenta esta situación, y con el fin de evitar futuros posibles daños, en Colombia se ha estado creando y desarrollando, de manera normativa y jurisprudencial mecanismos de protección que salvaguarden el derecho del habeas data y el tratamiento de datos personales de cualquier persona que esté en Colombia, sin importar su nacionalidad.

En Colombia la protección de datos personales es un derecho fundamental que está incorporado en la Constitución de 1991, artículo 15, con el cual se le garantiza a cada individuo que habita en el territorio, sin importar la persona jurídica de naturaleza privada o pública, que sus datos personales serán protegidos. Es así como las redes sociales no son la excepción.

Puesto que esta información y el trato que se le da es un derecho que a cada usuario se le tiene que asegurar y se debe de realizar cierta vigilancia para que no corra riesgo dicha información, entidades como la Superintendencia de industria y comercio buscan proteger los derechos del consumidor de posibles riesgos como seria la filtración de los datos personales en una red social.

Por esto, este artículo busca evidenciar si Facebook ha cumplido con las exigencias normativas de Colombia frente a la protección de datos personales, estableciendo la forma de recolección de la información de las plataformas hacia los datos de los usuarios; para así conocer los mecanismos de protección de estos, desde una perspectiva jurídica.

Nos apoyaremos en el método deductivo indirecto, en donde compararemos las condiciones contractuales del servicio de Facebook con la política de protección de datos personales, para así establecer si hay o no una vulneración al habeas data en este tipo de contratos; se realizará el estudio de casos, a través de las resoluciones expedidas por las SIC y otras entidades en la vigilancia sobre el trato que se le da a los datos personales de los consumidores, y como legalmente está regulado en Colombia.

1. Nociones generales ¿Qué se entiende por información privada o sensible en Colombia frente a las redes sociales?

El artículo 15 de la Constitución Política de Colombia, consagra el derecho de habeas data, permeándolo con garantías como la intimidad, la información y el buen nombre pues:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (C.P., 1991, art 15).

La Corte Constitucional en Sentencia T-509-20 ha definido este derecho como un derecho autónomo o instrumento para proteger otras prerrogativas; es una garantía que salvaguarda la libertad de la persona, entendida no como la posibilidad de locomoción sin restricciones, sino como la extensión que se hace de ella en medios virtuales o físicos de acopio de datos personales, en los cuales es construida o proyectada a través de la diferente información que se ha recogido de sí. De ahí que también reciba el nombre del derecho a la "autodeterminación informática".

Los datos personales son en sí aquellos que constituyen la materialidad del derecho al habeas data. De aquí podemos inferir que estos datos permiten una identificación, bien sea plena o parcial, de una persona; motivo por el cual es información privada, que pese a las leyes y demás reglas de administración, las cuales se verán más adelante, son datos que tienen por propietario al titular de los mismos.

1.1 Alcance normativo de la ley 1581 de 2012

Enfocándonos en la normatividad colombiana, se encuentra la Ley 1581 de 2012, que como su primer artículo menciona:

(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido

sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Esta Ley regula en general la protección de datos personales, buscando una legislación más adecuada frente a un derecho fundamental que es el habeas data, con la idea de garantizar los datos personales que se encuentren registrados, pues en las bases de datos lo que se realiza son operaciones de almacenamiento, control, uso y entre otras (Vélez, 2021)

Además de lo anterior, es necesario establecer que la Ley define a los datos sensibles como:

Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como los que revelen el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales de derechos humanos o que promuevan intereses de cualquier partido político o garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Basándonos en la sentencia C-748 de 2011, la cual realiza el control de constitucionalidad de la Ley en cuestión, podemos establecer los siguientes contenidos de este derecho fundamental:

a. El derecho de las personas a conocer la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información.

b. El derecho a incluir nuevos datos con el fin de ser provea una imagen completa del titular.

c. El derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos.

d. El derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad.

e. El derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular.

Así mismo, en la sentencia C-748 la Corte además señala que, al ser hoy en día un mundo globalizado, los datos personales son aún más importantes, y explica que Europa ha sido pionera en entablar regulaciones frente a esta nueva necesidad, en donde dice que un país tercero que recibiera los datos personales deberá de tener como mínimo un adecuado nivel de protección. (CC, Sentencia-748/2011, Col.)

1.2. Clasificación de la información personal

Con respecto a la era digitalizada en la cual se vive cotidianamente y la necesidad del ser humano por crear conexiones con los demás,

es común que la mayoría de las personas hagan uso de redes sociales, las cuales tienen multiplicidad de funciones como compartir información, conocer personas, ser una forma de entretenimiento, entre otras.

Las redes sociales no solo afectan a los usuarios, sino que también interfieren en la estructura social. De la misma forma se ha afirmado que:

Una red social es un portal de Internet que permite a las personas construir un perfil público o semipúblico dentro de los límites de la plataforma que ofrece los servicios que suelen ser muy variados y generalmente están constituidas por un grupo de personas ligado por intereses comunes, abierto a compartir pensamientos, pero también pedazos de la propia vida: desde enlaces a sitios que consideran interesantes hasta las fotografías o los propios videos personales (Constante, 2013).

Teniendo en cuenta que las redes sociales son un centro de depósito informativo, nos corresponde clasificar los tipos de información que las personas disponen en estas plataformas, no sin antes precisar que las redes sociales son un conjunto de componentes interrelacionados, los cuales recolectan, manipulan y diseminan datos e información, para poder ser centros de retroalimentación.

El derecho a la intimidad garantiza que los individuos gocen un entorno de privacidad, no susceptible de la intromisión de agentes externos debido a que se contempla como un espacio vital de la autonomía personal. También se debe aclarar que esta información puede ser divulgada por autorización de la persona o por la existencia de una decisión judicial. Es por esto por lo que los tipos de información que tienen

a. La información de carácter privado: Se relaciona con la intimidad y privacidad de las personas, en medios digitales no es accesible al público y goza de un carácter de confidencialidad. (López, 2021).

b. La información de carácter público: Este tipo de información es accesible a todo el mundo y cualquier usuario puede tener fácil acceso a ella. (López, 2021).

c. Reservada o secreta: Es aquella que es personal, pero tiene estrecha relación con derechos fundamentales, se encuentra reservada a su órbita exclusiva. Por ejemplo, los datos sobre la preferencia sexual, credo ideológico, sus hábitos y entre otros. (Sentencia T-114-18)

Teniendo en cuenta lo anterior es importante señalar que en efecto la información representada en datos bien sea pública o secreta, revela un entorno de la persona. Dependiendo de la manipulación de esta información se puede afectar la intimidad personal, económica y social del individuo. La Sentencia C-602 de 2016 señala que el derecho a la intimidad comprendía la información reservada, la privada y la semiprivada, entendiéndose estas como:

a. Información privada: Esta información es del ámbito propio del sujeto, es decir aquella información que revela facetas importantes de la vida personal y económica del individuo.

Para este aspecto la Ley 1581 de 2012, en virtud del principio de confidencialidad estipula que las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos,

están obligadas a garantizar la reserva de la información, incluso después de finalizada la relación con las labores que comprenden el tratamiento.

b. Información semiprivada: Según la Ley 1266 de 2008, es aquella que no tiene naturaleza íntima, reservada, ni pública, y su conocimiento o divulgación puede interesar no sólo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como lo son el dato financiero y crediticio de actividad comercial o de servicios.

Se establece de esta manera, en el sentido en que esta información "ayuda a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país".

Así mismo, la Ley 1266 del 2008 señala en su artículo 10 parágrafo 2° "(…) En ningún caso se podrá consultar esta información para fines de toma de decisiones laborales, y no podrá utilizarse para fines diferentes al análisis o cálculo del riesgo crediticio del titular del dato".

c. Información reservada: La ley 1755 del 2015 en su artículo 24 establece 8 informaciones y documentos reservados, los cuales están relacionados con la defensa o seguridad nacionales; las instrucciones en materia diplomática o sobre negociaciones reservadas; los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales; los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la nación; los datos referentes a la información financiera y comercial, en los términos de la Ley Estatutaria 1266 de 2008; los protegidos por el secreto comercial o industrial, así como los planes estratégicos de las empresas públicas de servicios públicos; los amparados por el secreto profesional; y los datos genéticos humanos.

Así mismo, la Ley 1712 de 2014 señala que la información pública reservada es aquella información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos. Como ejemplo de esto podemos encontrar el "índice de información clasificada y reservada" de la Fiscalía General de la Nación, en donde tienen como carácter de reserva las órdenes de trabajo debido a la constatación de datos personales, privados y semiprivados de las personas, cuya divulgación puede generar un daño en los derechos a la intimidad, la vida, la salud o la seguridad de las mismas.

Sin embargo, estos listados no son taxativos, pues la información versa sobre aquellos datos que tienen estrecha relación con los derechos fundamentales de dignidad humana, intimidad y libertad en estricto sentido, aunque gran parte de esta información es limitada por disposición constitucional o legal.

El ordenamiento jurídico colombiano, si bien nos cataloga la información privada en la ley 1581 de 2012 para la protección de datos personales,

desarrolla la protección constitucional del Habeas Data; no por estar catalogados nos ofrece una taxatividad normativa, pues el propósito de la norma es proteger la información del ámbito propio de las personas, las cuales revelan particularidades de la intimidad personal, social y económica de estas.

Se puede concluir que en el mundo la mayoría de los países utilizan y dependen de las redes sociales, haciendo parte del diario vivir. Frente a esto, en Colombia se ha venido implementando de manera normativa, como lo es la ley 1581 de 2012, y también por medio de jurisprudencia de la corte constitucional, la protección de datos personales o habeas data como un derecho fundamental, y más en la modernidad con el tema de la virtualidad.

2.Términos contractuales de Facebook

Para que una persona se obligue jurídicamente, es necesario que haya una manifestación expresa de su voluntad. El contrato es aquel instrumento que acoge las necesidades prestacionales de las partes; con base a esto, cabe preguntarnos, ¿aceptar los términos y condiciones de Facebook que representa en el marco contractual colombiano?

Si bien es cierto que Facebook establece un contrato de adhesión, que busca satisfacer las necesidades de consumo privado en su generalidad, este tipo de contrato reviste características especiales, en el sentido en que no es nominado en el ordenamiento jurídico; es por esto que para entender el contrato lo vamos a clasificar según la distinción clásica de los contratos.

Clasificación	¿Por qué?
Innominado	Esto debido a que carece de una regulación especial, pero se debe ceñir a los principios generales del derecho, su interpretación se basa en la analogía, a los pronunciamientos judiciales y a la normativa del sector. Es decir, su estructura y efectos no tienen una determinación normativa.
Unilateral	Facebook se compromete a disponer su plataforma a los usuarios, sin que estos tengan una contraprestación por el uso de esta. No se generan obligaciones contra prestacionales recíprocas
Gratuito	No hay una utilidad por la prestación; sin embargo, "hay un debate doctrinal sobre el valor monetario en el uso que dan las aplicaciones a los datos personales recolectados para crear ventajas comparativas empresariales" (Moreno, 2022). Esto se debe tener en cuenta debido a que Facebook nos condiciona a que la información que recopila, la transfiere a proveedores generales y de servicios en todo el mundo para poder mantener el negocio; es decir, "la información de los usuarios es un instrumento negociable para financiar estudios y estrategias de mercadeo para utilizarlas con los usuarios de la plataforma, sus subsidiarias, terceros y esto sin que el usuario se beneficie económicamente ya que el usuario cedió ese derecho" (Gierbolini, 2017).
Principal	Subsiste por sí mismo, en el sentido en que no asegura ni se deriva de una obligación principal.
Perfección solemne	Se perfecciona con el acuerdo de voluntades manifestado al hacer click en el aceptar de los términos y condiciones de la aplicación
De adhesión	Hay una imposición del contenido contractual, situando a Facebook como la parte fuerte del contrato ya que determina las condiciones de este. El usuario no puede discutir las cláusulas contractuales, solo puede otorgar o no permisos en cuanto a su privacidad.
De ejecución sucesiva.	Su objeto contractual se ejecuta en actos escalonados, debido a que no hay un único momento para cumplir la obligación principal la cual es de prestar un servicio, dicho servicio no establece una modalidad especifica de duración, permanencia o modo de acceso para iniciar la aplicación.

Elaboración propia. Información obtenida de Peña (2013).

Entendiendo que el contrato de Facebook sitúa a la aplicación en una obligación de ejecutar el programa para que el usuario se beneficie, en donde la obligación es de carácter sucesivo, la cual busca satisfacer las necesidades de consumo privado; algunos escritores determinan a este tipo de contratos (aquellos de aplicaciones en general) como contratos de suministro. Sin embargo, "en términos del artículo 968 del Código de Comercio, el contrato de suministro es oneroso, pues requiere de una contraprestación; teniendo en cuenta que muchas aplicaciones que prestan a los usuarios un servicio gratuito, hay un debate doctrinal sobre el valor monetario en el uso que dan las aplicaciones a los datos personales recolectadas para crear ventajas comparativas empresariales" (Moreno, 2022).

Podemos establecer que el contrato de Facebook con los usuarios puede que no sea el único en el mundo en cuanto a su tipología, en el sentido de que otras aplicaciones usan estos elementos para desarrollar su objeto contractual. Sin apartarnos de nuestro tema de estudio, lo anterior es importante para establecer que en efecto, Facebook tiene obligaciones contractuales, las cuales no son menores y se deben ceñir a la ley sin importar que el usuario no genere contraprestaciones, pues lo realmente relevante en el caso es que el usuario le está brindando información personal a una plataforma que tiene el deber contractual y legal de brindar seguridad a esos datos.

3. Sobre la recopilación de datos en las aplicaciones

Globalmente Facebook es reconocida como una de las aplicaciones sociales con más usuarios registrados, pues si bien empezó siendo una aplicación para estudiantes universitarios, tuvo un crecimiento exponencial por su facilidad para compartir y conocer personas en línea. Facebook "es una empresa de origen estadounidense con sede en California-EE. UU. Que ofrece servicios de redes sociales en línea. Aunque en su origen surgió como sitio web para los estudiantes de Harvard gradualmente fue expandiendo su ámbito de funcionamiento" (Rodriguez, 2021, pág. 38).

Continuando con "la política de expansión de Facebook siguió en la misma línea, convirtiéndose en una red que cada vez agrupaba más usuarios, girando en torno a estudiantes de distintas instituciones. En septiembre de 2006, el servicio se abrió a todo público" (Roa, 2013, pág. 70)

Debido a esta popularidad, Facebook evoluciona a tal punto que se vuelve una empresa a nivel global, en el cual afirma que cualquiera puede ser usuario de su red social de manera gratuita; sin embargo, la BBC en su reporte del 25 de marzo del año 2018 señaló que: "la red social invade la privacidad de sus usuarios con el fin de obtener dividendos para la compañía". En septiembre de 2018 la Comisión Europea dio un ultimátum de tres meses a Facebook para que adaptara sus prácticas a la normativa de consumo de la UE. Bruselas también "amenazó con sanciones a la red social estadounidense en caso

de que sus términos y condiciones siguieran sin regirse por las leyes europeas de protección de los consumidores" (Rodriguez, 2021, pág. 42)

La empresa que administra Facebook y otras redes sociales hoy en día se le conoce como Meta, la cual, en sus páginas oficiales, ha dicho "La información que recopilamos y tratamos sobre ti depende de la forma en la que usas nuestros Productos. Por ejemplo, recopilamos información diferente si vendes muebles en Marketplace o si publicas un reel en Instagram. Recopilamos cierta información sobre ti cuando utilizas nuestros Productos".

3.1. Información que Recopila Meta

Como lo explica Meta (2022), desarrolla su tecnología y servicios con la idea de que las personas se puedan conectar, crear comunidades e incluso hacer negocios. Estas condiciones rigen en Facebook, Messenger y otros productos de la empresa, excepto cuando se llegue a indicar lo contrario de manera expresa. Por una parte, no se hace ningún cobro al usuario por usar Facebook y demás productos que estén relacionados a las dichas condiciones, pero por el otro lado se encuentran organizaciones, negocios e incluso personas que pagan para mostrar anuncios de sus productos y servicios. Esto se debe a que, al usar los distintos productos de Meta, dentro de los términos y condiciones de uso de las aplicaciones el usuario acepta que le sean mostrados dichos anuncios, los cuales son personalizados y adecuados a las diferentes preferencias que tiene el individuo, y al uso que este haga de la red social; es decir, los anuncios que aparecen dependiendo del perfil de cada persona son de productos que dicha persona es más propensa a comprar.

Meta, en su página "Condiciones y Política", aclara que no venden los datos personales de los usuarios a los anunciantes, ni comparten información como lo es el nombre, dirección del correo electrónico u otra información de contacto a los mencionados anunciantes, sino que estos últimos proporcionan datos como el tipo de público que quieren que vea sus anuncios, y Meta Proporciona informes a estos anunciantes para que vean el rendimiento de su publicidad con el público.

A continuación, se mostrará con el siguiente esquema cuales son los datos que recopila y la forma de cómo los recopila la Empresa Meta (Facebook, WhatsApp e Instagram). Se debe de tener en cuenta "que la actividad es todo lo que uno puede hacer a través de los productos e información que proporciona Meta" (Meta, 2023).

¿Qué información recopilan?	¿Cómo la recopilan?
La actividad e información que el usuario proporciona	Como lo menciona Meta (2023) en su política de privacidad. • Contenido creado; publicaciones, comentarios, entre otros • Contenido por medio de la cámara y galería o mediante funciones de voz, se recopila para máscaras, efectos, filtros, avatares • Tipos de contenido que uno ve o con el que interactúa y la manera en que se hace • Compras u otras transacciones que se realizan, incluida la información de la tarjeta de crédito. • Entre otras

¿Qué información recopilan?	¿Cómo la recopilan?
A través de la interacción de amigos, seguidores, y otras conexiones	Como lo menciona Meta (2023) en su política de privacidad. • Recopilan la información sobre amigos, seguidores, grupos, cuentas, páginas de Facebook y otros usuarios y comunidades con los que uno se conecta e interactúa • También recopilan los contactos, como son el nombre y la dirección de correo electrónico o un número de teléfono, y uno elige si subirla o importarla desde un dispositivo como al sincronizar la libreta de direcciones • La formación que recopilan o infieren de uno en función de la actividad de otras personas; como las sugerencias de amistad y de grupos
Mediante información de la app, el navegador y el dispositivo	Como lo menciona Meta (2023) en su política de privacidad. • Recopilan y reciben información de los diferentes dispositivos que uno usa, la manera en que se usa, y datos sobre dichos dispositivos. De la siguiente manera: • El dispositivo y el software que uno está usando, y otras características del dispositivo. • Lo que uno está haciendo en el dispositivo por ejemplo cuando uno está en la página y está moviendo el ratón (dicha acción permite distinguir a los humanos de los bots). • identificación entre el dispositivo de uno y los de más usuarios, incluyendo los familiares • Información que uno comparte con la página a través de la configuración del dispositivo, como ubicación GPS, acceso a la cámara, fotos. • Información sobre la red a la que uno se conecta por medio del dispositivo, incluida tu dirección IP. • Información sobre el rendimiento de los Productos de la empresa en el dispositivo. • Información de cookies y tecnologías similares.
Por medio de la información de socios, proveedores y terceros	Como lo menciona Meta (2023) en su política de privacidad • Información del dispositivo de uno. • Sitios web que uno visita y datos de cookies, por ejemplo, por medio de plugins sociales o el píxel de Meta. • Apps que usamos, aplica en los juegos también • Compras y transacciones que uno realiza. • Datos demográficos, como nivel de formación. • Anuncios y cómo uno interactúa con ellos. • Cómo uno usa los productos y los servicios de los socios online (De Meta) o en persona.

Elaboración propia. Información obtenida de la página Política de privacidad De Meta

En el caso de datos personales que son delicados, Meta menciona en su página Política de privacidad, ¿Qué es la Política de privacidad y qué cubre? que está vigente desde el 1 de enero de 2023, que "Podrías elegir proporcionar información sobre creencias religiosas, orientación sexual, ideologías políticas, salud, raza, origen étnico, creencias filosóficas o pertenencia a sindicatos. Estos y otros tipos de información podrían tener protecciones especiales en virtud de la legislación de tu jurisdicción."

Cómo se puede ver en el anterior cuadro hay varias formas de cómo se recopilan los datos personales de una persona, esto teniendo en cuenta la legislación de cada país.

La manera de como usan la información que recopilan o recolectan de cada uno de los usuarios, lo usan para lo siguiente según en su página de Política de privacidad

- Para proporcionar, personalizar y mejorar sus productos
- Para fomentar la seguridad, la protección y la integridad
- Para ofrecer servicios de medición, de análisis y comerciales
- Para mantener una comunicación con el usuario
- Para realizar investigaciones e innovar para el bienestar social

Facebook asegura que brinda seguridad al usuario en sus términos y condiciones. En cuanto a la protección de datos personales, nos indica cómo esta empresa obtiene ganancias al ser ella misma la que organiza y filtra el tipo de contenido y ámbitos promocionales que se le ofrecen a los usuarios dentro de la aplicación, enfatizando en que los datos no se venden.

4. Mecanismos de protección de los usuarios de Facebook

4.1. Mecanismos de protección de los datos personales de los usuarios de Facebook dentro de la red social

Meta, aparte de sus políticas de privacidad, también cuenta con su centro de privacidad en el cual menciona lo siguiente "Elige las opciones de privacidad que consideres adecuadas para ti. Obtén información sobre cómo administrar y controlar tu privacidad en Facebook, Instagram, Messenger y otros productos de Meta" (Meta, S.F.)

En esta página te encuentras guías como; Cómo protegerte a ti mismo y a tu información, Mantener la seguridad de tu información protege tu privacidad, Información sobre la privacidad para adolescentes, entre otros

La guía de cómo protegerte a ti mismo y a tu información nos menciona que "Consulta herramientas importantes que pueden ayudarte si quieres limitar quién puede interactuar contigo o ver lo que compartes" (Meta).

Pasos para proteger tu información	Método de proteger tu información
Limita quién puede ver lo que compartes	Como lo menciona Meta (2023) en su página Centro de Privacidad" "Para proteger tu privacidad, tienes la posibilidad de limitar lo que determinadas personas pueden ver. Puedes administrar más opciones de privacidad en el menú de configuración de Facebook, Instagram y Messenger"
Protege tus mensajes y otra información privada	Como lo menciona Meta (2023) en su página Centro de Privacidad "Es posible que, en ocasiones, te preocupe especialmente que otras personas puedan ver información de tus cuentas, por ejemplo, si crees que alguien podría saber tu contraseña o si perdiste el acceso a tu dispositivo." Métodos que puede usar para proteger tu cuenta y tu información • App de autenticación • Mensaje de texto (SMS) • Llave de seguridad
Obtén ayuda si sientes que eres víctima de acoso o bullying	Como lo menciona Meta (2023) en su página Centro de Privacidad "Descubre las herramientas que están a tu disposición, por ejemplo, cómo bloquear a alguien o cómo reportar una situación de acoso"

Elaboración propia. Información obtenida de la página Centro de Privacidad de Meta

Frente a estos mecanismos de protección se puede analizar cierto interés de Facebook por brindarles herramientas a sus usuarios, con el fin de proteger su intimidad y privacidad en contra de terceros

En el caso del primer mecanismo busca que el usuario pueda limitar o restringir el acceso de su información a otros usuarios que le puedan afectar su información.

Mientras que, en el segundo paso, se enfoca en el acceso del perfil o cuenta del usuario, en donde busca proteger su ingreso de terceros no deseados.

Y el último paso da mecanismos en relación con las políticas de la comunidad, en donde se busca evitar alguna discriminación a la información sensible u otra que pueda poner en riesgo al usuario usando herramientas como el bloqueo

La otra guía que es de nuestro interés para el artículo sería "Mantener la seguridad de tu información protege tu privacidad", en el cual se menciona que "Queremos ayudarte a comprender cómo puedes usar nuestras funciones de seguridad para agregar un nivel de protección adicional a tus cuentas" (Meta, S.F).

En esta guía se menciona cómo se combate el uso indebido de datos, donde mencionan que "Nos esforzamos mucho para proteger tu información. Tenemos un equipo dedicado a combatir el uso indebido de datos externos (compuesto por científicos, analistas e ingenieros) que nos ayuda a detectar, bloquear e impedir la extracción de datos" (Meta, S.F), dándonos a entender que Meta busca tener un sistema de base de datos que pueda proteger y garantizar la intimidad y la privacidad de sus usuarios, o al menos dejando ver que tiene una normatividad interna dentro de la empresa frente a este tema y de como lo ha ido regulando.

4.2. Mecanismos de protección de los datos personales de los usuarios de Facebook bajo el derecho colombiano

La eventual vulneración de cualquier derecho presupone un mecanismo el cual garantice la protección de este, pues con la Constitución de 1991 nos establecemos como un Estado social de derecho que se funda en la dignidad humana, y por esto es que el Estado tiene el deber de proteger los derechos y libertades de todos los residentes en el país.

Teniendo en cuenta lo anterior, se crean diversos mecanismos de protección de derechos; mecanismos que pueden ser articulados per se para que la efectividad del derecho, y el acceso a la justicia, sea oportuna. Algunos de estos mecanismos son el derecho de petición, el habeas corpus e incluso la tutela. Pero recordemos que hay otro mecanismo que se enfoca directamente en la protección de los datos personales, que se encurta como un derecho fundamental, siendo el artículo 15 de la constitución del 91, el Habeas Data.

Si bien es cierto que hemos tomado como norma rectora para la protección de datos personales la Ley 1581 del 2012, debemos de centrarnos y recordar que el habeas data es un derecho fundamental personalísimo que refiere

al honor, la intimidad, la imagen y la dignidad humana; es por esto por lo que independientemente de la autorización que se le haya generado a la fuente de información (base de datos), es el titular de la información el propietario de sus datos.

Cuando el usuario evidencia una vulneración en su información por ser incierta o desfavorable, puede apelar a su derecho del habeas data mediante una queja, denuncia, entre otros medios directos ante el responsable del tratamiento de sus datos; este reclamo se hace mediante derecho de petición, pues sin importar que el operador de la información sea una persona pública o privada, con o sin personería jurídica, tiene el deber de garantizar la protección de los derechos fundamentales, pues de negarse a la recepción o contestación del mismo, puede enfrentarse a sanciones.

Cuando la respuesta al derecho de petición por parte del operador genere aun inconformidad, o no se haya generado respuesta alguna, el usuario podrá recurrir a la Superintendencia de Industria y Comercio para que se impongan sanciones conforme a la Ley y se adopten decisiones que hagan efectivo el derecho al Habeas data.

Lo anterior entendiendo que la Superintendencia de Industria y Comercio es una entidad pública de carácter nacional, adscrita al Ministerio de Comercio, Industria y Turismo de Colombia, es la autoridad nacional de protección de la competencia, los datos personales y la metrología legal; con las Leyes 1266 de 2008 y la 1581 de 2012 2012 se le otorgan facultades a esta entidad para vigilar a los operadores, fuentes y usuarios de información. Estableciendo así que es una entidad que protege y promueve los derechos de los consumidores a nivel nacional.

Como última alternativa, y en el caso inusual en el que la SIC no haya podido garantizar efectivamente el derecho del habeas data al usuario, se podrá interponer una acción de tutela, recordando que esta es una acción subsidiaria, la cual no puede ser ejercida de forma temeraria.

La garantía de este derecho fundamental genera una certeza de protección, no solo por las acciones que el usuario per se pueda ejercer, sino por aquellas facultades coercitivas que la Ley brinda a la SIC para aquellos casos en el que la vulneración a los datos personales por parte de los operadores sea flagrante.

4.2.1. Herramientas para solicitar la intervención de la SIC

Herramientas	Contenido
Demanda	Quien demande, tiene como objetivo el cambio o reparación del bien, cambio, devolución, etc Esta acción judicial busca proteger al consumidor, aunque también se puede para indemnizar por perjuicios en relación a la publicidad engañosa, Esta acción se dirige contra el proveedor, comercializador y/o fabricante
Denuncia	El objetivo de la actuación es proteger el interés general y el derecho colectivo de todos los consumidores. Esto por medio de la denuncia, en donde el consumidor busque que la SIC, comience una investigación administrativa al proveedor, comercializador y/o fabricante. En este proceso el denunciante no obtiene ninguna forma de reconocimiento de manera particular y mucho menos obtiene la solución del caso individual.

Elaboración propia. Información obtenida de la página oficial de la SIC

Lo que se busca con estos mecanismos es proteger al consumidor, esto debido a que es la parte débil en estos temas.

En la página de la SIC menciona que estos mecanismos se pueden aplicar en temas de información personal "Habeas data" sobre; Operadores y fuentes que tengan información de personas, Corrección, actualización o retiro de datos.

5. El rol de la Superintendencia de Industria Y Comercio (SIC)

Para iniciar este capítulo se debe de tener en cuenta qué es la Superintendencia de Industria y Comercio (SIC), la cual de manera directa desde su página oficial menciona que "es la autoridad nacional de protección de la competencia, los datos personales y la metrología legal, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial, a través del ejercicio de sus funciones administrativas y jurisdiccionales."

Enfocándonos en la parte de la protección de datos, la SIC en su página oficial menciona que busca "Garantizar que, en la recolección, el uso, la circulación y el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley (Derecho al debido tratamiento de datos personales)" esto en aras de cumplir y proteger el artículo 15 de la constitución política de Colombia.

Todo esto, basado en la Ley 1581 de 2012 que le otorga la competencia a la SIC por medio de la creación de una delegatura, cuya función es garantizar el cumplimiento de las disposiciones normativas sobre el tema de manera efectiva.

Una de las facultades de la SIC es dar diferentes tipos de sanciones como las pecuniarias "a los responsables del tratamiento de datos que no cumplan las políticas de protección establecidas en la ley, las cuales consisten en multas, suspensión de actividades y suspensión definitiva de las operaciones en caso de que involucren tratamiento de datos." (Rojas, 2014, pág. 120)

Sin embargo, la SIC también se ha encargado de tener un rol de asesor y de ayudar de diferentes formas, como la expedición de guías, cuestionarios y formatos que tienen como objetivo aclarar y facilitar el cuidado de datos personales, tanto a personas jurídicas de naturaleza pública o privada; algunas de estas guías son: la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) del 2016, formato modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios del 2017, Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes del 2018, Guía para la implementación del principio de responsabilidad demostrada del 2019. Estos documentos, entre otros, tienen como objetivo orientar a las personas jurídicas que administran, recolectan y adquieren datos personales.

5.1. Sobre el "accountability"

El decreto 1377 de 2013, el cual reglamenta la Ley 1581 de 2012; establece el principio de "accountability". Este es un principio con el cual aquellos responsables del tratamiento de datos personales deben estar sometidos al cumplimiento general de protección de los mismos ante la Superintendencia de Industria y Comercio, y esto se logra a través del poder demostrativo de la implementación de medidas apropiadas y efectivas para el cumplimiento de lo estipulado en la Ley 1581 de 2012; además de esto señala:

(…) En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

Las políticas internas que deben de adoptar los responsables del tratamiento de datos personales son de acuerdo con la naturaleza jurídica del responsable, a la naturaleza de los datos objeto del tratamiento, el tipo de tratamiento y los riesgos potenciales sobre los derechos del titular. Esto se garantiza a través de la debida diligencia de la estructura administrativa, la cual debe ser capaz de adoptar mecanismos de protección, así como la puesta de procesos para la atención de consultas, peticiones y reclamos de los titulares.

Este programa de gestión de datos personales debe garantizar una eficacia permanente. Es por esto por lo que el decreto 1377 de 2013 establece que debe haber una persona o un área encargada que asuma la protección de los datos personales. Este a su vez se encargará de la revisión y establecimiento de medidas de desempeño de manera anual sobre la recolección de datos personales; así mismo, establecerá las amenazas y riesgos al tratamiento de los datos personales detectados en la organización, si se están ofreciendo nuevos servicios que involucren mayor recolección de información personal o si se está llevando la captación de acuerdo con el procedimiento establecido el cual debe estar en constante actualización.

Con base a estas especificaciones es que los responsables podrán demostrar ante los titulares y ante la Superintendencia de Industria y Comercio que existe una adopción de un programa específico para la gestión de datos personales los cuales cumplen la normatividad de protección. Pues de no ser capaz de demostrar la correcta aplicación de protección a los datos personales, la SIC evalúa la imposición de una sanción de acuerdo con las especificaciones que debe tener la empresa para la recolección de los mismos.

5.2. Sobre el formato modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios

Las personas tienen el derecho de conocer, actualizar y rectificar sus datos personales; derecho que no solo se establece en la Constitución Política de Colombia en su Artículo 15, sino que también en la ley 1581 del 2012, en el cual genera unas obligaciones a toda persona que administre datos personales.

En base a esto, la SIC crea el "el Formato modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios" dejándolo a disposición de los interesados con el objetivo de facilitar el cumplimiento de la ley 1581 de 2012, el cual los interesados deben cumplir con ciertas obligaciones como lo serían:

I. Solicitar y conservar copia de la autorización otorgada por los titulares para el tratamiento de su información personal y de la información que debe suministrársele a estos,

II. Contar con una política de tratamiento de información personal que debe estar disponible para los titulares y

III. Contar con un aviso de privacidad, cuando no sea posible poner a disposición de los titulares directamente, la política de tratamiento.

En esta cartilla se explica que la autorización es un tema relevante para el tratamiento de datos personales, la cual trata sobre el consentimiento de una persona en cuanto al trato de sus datos personales que va dar a alguien sea una persona natural o una empresa. Sin embargo, quienes están recopilando los datos pueden solicitar el consentimiento al titular, y este último para dar su aprobación debe saber el cómo y para que se va a utilizar su información, y a su vez tener la posibilidad de realizar consultas a futuro.

Para obtener esa autorización, se puede de manera escrita, oral o "Mediante conductas inequívocas del titular de la información, las cuales permiten concluir a los responsables que se otorgó la autorización." La cartilla menciona que para poder recoger esa información se debe de tener un fin coherente, claro y preciso.

6. Vulneración al Habeas Data en Facebook

Teniendo entendido que el Habeas Data es una garantía constitucional que permite la protección a la intimidad personal, debido a que la persona es quien tiene la posibilidad de preservar del conocimiento público información propia y en caso de querer revelarla ante administradores de datos, se debe hacer mediante manifestación expresa e inequívoca y que pese a lo anterior tiene el derecho de incluir, excluir, corregir o actualizar los mismos; cabe retomar la pregunta de ¿Hay una vulneración en el habeas data de los contratos de usuario de Facebook? Para responder esto nos enfocaremos en las condiciones y políticas de privacidad de Facebook contrastándola con la Ley 1581 del 2012.

6.1. Condiciones del servicio "Declaración de derechos y responsabilidades"

Las condiciones de Facebook hacen referencia a la manera en cómo la aplicación usa y comparte los datos de los usuarios. Cabe mencionar que estas condiciones no solo hacen referencia al uso dentro de Facebook sino a todos los productos de Meta

En cuanto a los anuncios, Meta menciona que no se venden los datos personales a los anunciantes ni se comparte la información que identifique directamente a la persona, es decir lo que catalogamos como información privada. Lo que hace Meta es analizar los aspectos objetivos comerciales de los anunciantes y el tipo de público que quieren que vea los anuncios y así, Meta personaliza el mismo. Es importante mencionar que existe la posibilidad de que Meta sí comparta la información de contacto, siempre y cuando el usuario dé su permiso expreso.

Ahora bien, los anunciantes lo que reciben de los usuarios son datos demográficos generales, los cuales no generan una identificación directa de la persona. Sin embargo,

hay un punto que llama la atención y es que esta información privada puede ser compartida si se da el permiso expreso. Lo que debemos tener en cuenta aquí es que en efecto el titular puede disponer de su información, y Facebook se supone que garantiza el derecho del habeas data al pedir autorización previa y expresa, pero ¿para el usuario habrá claridad de esta autorización cuando simplemente presiona el botón de "autocompletar" cuando ingresa a un anuncio?

Por un lado, podríamos evidenciar un grado de contradicción frente a las acciones que se realizan con los anuncios, pues Facebook tiene la autorización de mostrar al público los intereses de contenido comercial a los cuales hemos recurrido.

Al aceptar las condiciones de Meta, la empresa tiene la información de todo lo que se hace dentro de sus productos, pero también aceptamos que puede recolectar la información de "lo que haces fuera de nuestros productos". Puede llegar a ser preocupante este punto en el sentido en que, en efecto, Facebook lo único que necesita es autorización expresa para acceder a la información de nuestros dispositivos, pero ¿Qué tanta información recolecta?, esto es algo que trata de ampliar en política de privacidad, la cual veremos más adelante, y decimos trata porque lo único que nos menciona son ejemplos.

Así mismo, estamos aceptando que Facebook comparta información con las empresas de Meta que proporcionan productos y servicios financieros, pues lo que busca es "fomentar la protección, la seguridad y la integridad, y a cumplir con la legislación aplicable". Nos menciona además que Meta puede acceder, conservar, usar y compartir cualquier información que recopile sobre el usuario cuando "crea de buena fe que esto es algo que la ley permite o exige. Para obtener más información, consulta nuestra Política de privacidad".

Aquí debemos tener en cuenta dos puntos: el primero es que Meta debe garantizar que los operadores de información (recordemos que son aquellos que reciben información de la fuente de datos y administra dicha información) garanticen el cumplimiento de los deberes y responsabilidades de la protección de datos personales; y el segundo punto es que si bien Facebook es una aplicación en la que se pueden realizar actividades comerciales, ¿Por qué es pertinente la recopilación de estos datos reservados? Esto teniendo en cuenta que, si es por la personalización de los anuncios, estos datos no son relevantes, pues lo que los anunciantes necesitan son datos demográficos generales que no relacionan directamente a la persona y lo que hace Facebook para la personalización es buscar los patrones de interacción con sus productos; anudado a que, en su política de privacidad, no menciona cuáles son sus productos o servicios financieros.

Por otro lado, como usuarios permitimos que en el momento en que compartimos, subimos o publicamos contenido, este se determine como información pública que se difundirá conforme a nuestros permisos de público dentro de la aplicación. A su vez, Facebook contará con licencia para su almacenamiento y publicidad. Cabe aclarar que esta termina cuando el usuario decide eliminar el contenido.

Frente a las obligaciones de garantizar la recolección, tratamiento y la circulación de datos, Meta menciona que, según las actualizaciones en sus productos, la optimización de sus servicios y sus nuevas funciones, existe el deber de actualización de condiciones para que "reflejen con precisión nuestros servicios y nuestras prácticas, así como para promover una experiencia segura y protegida en nuestros Productos y servicios, y para cumplir con la ley aplicable". La empresa se obliga a enviar al menos con 30 días de anterioridad a la modificación de las Condiciones, las mismas para que pueda el usuario conocerlas. Ahora bien, la aceptación de estas modificaciones es tácita, pues no hay una aceptación expresa del usuario en el sentido en que son aplicables si el usuario sigue haciendo uso de la aplicación y en caso de no estar de acuerdo, el usuario debe eliminar la cuenta para que estas no se apliquen "si no aceptas nuestras Condiciones actualizadas y ya no quieres formar parte de la comunidad de Meta, puedes eliminar tu cuenta en cualquier momento".

6.2. Centro de Privacidad

En Meta aparte de las políticas de seguridad, está el centro de Privacidad donde se tratan varios temas frente a la información de los usuarios como seria, "Protégete a ti y blinda tu información", en el cual se menciona que tiene herramientas para poder limitar la información del usuario, y en relación de la red social Facebook está la autenticación de dos pasos, y Limitar quién puede ver lo que compartes; sin embargo, no son mecanismos totalmente eficientes en la protección de datos personales, pues si bien se puede limitar la información a ciertos usuarios, no garantiza su protección, debido que ese usuario que fue limitado puede crear otra cuenta y seguir invadiendo la privacidad de la persona.

Otro subpágina que se encuentra en el centro de privacidad es "Mantener la seguridad de tu información protege tu privacidad" donde se menciona que se puede proteger la cuenta de un usuario aún más, en el caso de Facebook, con solicitudes de inicio de sesión, que consisten en el envío de una notificación sobre la ubicación y el nombre de un dispositivo desconocido, desde el que se busca ingresar a la cuenta del usuario. Dicha medida carecía de eficacia, debido a que depende mucho que el dispositivo desconocido tenga activada la opción para encontrar su ubicación exacta. También está tu contraseña, pestaña en la cual se puede crear una contraseña, con un requerimiento mínimo de caracteres, entre letras mayúsculas y minúsculas, números y teclas especiales.

Por otro lado, se encuentra la Herramientas y políticas de seguridad, en la cual la página menciona que la herramienta "Manténgase seguro" busca que el usuario aprenda de temas tales como el control sobre cómo hacer amigos, compartir su información personal y denunciar contenido que viole nuestras políticas.

Esta segunda herramienta que es "Asegure su cuenta" tiene la finalidad de establecer contraseñas seguras y utilizar herramientas de inicio de sesión, como la autenticación de dos factores. Incluso también está la opción de qué hacer si cree que su cuenta ha sido pirateada o necesita informar problemas de seguridad.

Y la última herramienta que es "Proteja la información personal" trata de cómo se puede tener un control sobre quién ve las publicaciones, y qué información está disponible para la vista del público, además de administrar las etiquetas de las publicaciones.

Si bien estas herramientas son más eficaces que las mencionadas anteriormente, su uso y manejo no es tan sencillo para el usuario debido a que estas herramientas se encuentran en "Herramientas y políticas de seguridad". Sin embargo, la principal idea de la creación de estas herramientas es que cuenten con una interfaz y un menú de opciones interactivo y fácil de comprender para el usuario. Lastimosamente, debido al inadecuado y complejo diseño de estos apartados, el usuario tiene que rebuscar en una cantidad de opciones que dificultan su uso, llegando al punto de poder sentirse abrumado, además de no tener la posibilidad de acceder a, o encontrar dichas herramientas.

7. Sobre las actuaciones de la SIC hacia Facebook

Con base al principio de accountability y el Formato modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios, deja en claro que la SIC busca una garantía a la protección de datos personales de los usuarios. La Ley 1581 de 2012 en su artículo 21 faculta a la SIC para impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones; es por esto por lo que dicha entidad ha expedido diversas resoluciones, las cuales garantizan la adopción de medidas específicas en empresas para la gestión de los datos personales. Debido a su importancia destacaremos la Resolución 1321 de 2019.

No. de Resolución	**Resolución 1321 de 2019**
Entidad emisora	Superintendencia de Industria y Comercio
Fecha	24 de enero de 2019
Radicado	18-233402
Investigado	Facebook Colombia SAS
	Facebook INC
	Facebook Ireland Limited
Asunto	Por la cual se imparten órdenes dentro de una actuación administrativa.
Hechos	1. El 19 de diciembre de 2018, el fiscal General para el Distrito de Columbia en Estados Unidos, descubrió lo siguiente:
	• En el 2013, Facebook permitió a Aleksandr Kogan, un investigador afiliado a la Universidad de Cambridge, y su compañía "GSR" que operara una aplicación llamada "thisisyourdigitallife" en la plataforma. Esta aplicación generaba un perfilamiento a cambio de que los usuarios descargaran la aplicación y autorizaran el acceso a la información de sus cuentas en Facebook.
	• Los datos recolectados se relacionaban con el nombre, género, fecha de nacimiento, ciudad actual y "like".
	• La aplicación recolectó la información de los amigos de los usuarios que la descargaron en Facebook, aunque esas personas no habían otorgado permisos a la aplicación para compartir su información personal.
	• En el año 2014, la compañía "GSR" vendió la información personal recolectada a Cambridge Analytica, incluyendo los datos de millones de personas que nunca descargaron la aplicación ni otorgaron su consentimiento para el tratamiento de sus datos.
	• Cambridge Analytica y sus clientes usaron la información para propósitos políticos en la campaña presidencial en el año 2016 de los Estados Unidos, en función de su perfilamiento.
	• A pesar de que Facebook conocía que la información personal de millones de sus usuarios fue recolectada y vendida en el año 2015, esperaron más de dos años para comunicar el incidente ocurrido.
	2. El anterior reporte fue publicado por el diario "The Guardian", y con base a esto la dirección de investigación de protección de Datos personales decidió iniciar indagación preliminar contra Facebook.
	3. El día 26 de marzo de 2018, la dirección de investigación realizó una inspección en las instalaciones de Facebook Colombia SAS, con el fin de verificar el cumplimiento de la normatividad en protección de datos personales.

Investigación	Facebook, debido a la investigación inicia por la SIC, precisó lo siguiente:
	● No se cuenta con un departamento administrativo y todos los servicios legales están tercerizados y solo se hacen reportes comerciales a la casa matriz.
	● Respecto de la seguridad de los datos personales afectados en el incidente que involucra a Facebook y Cambridge Analytica, dichos temas están centralizados en Estados Unidos.
	Entre otra información solicitada por la SIC, la cual tiene un carácter reservado, la entidad concluye que:
	● Facebook recolecta y trata datos personales de más de 31 millones de colombianos.
	● Facebook usa y circula los datos de manera global y transfronteriza.
	● Pese a las "políticas, herramientas y recursos para proteger los datos personales", Facebook no ha adoptado medidas de seguridad suficientes y efectivas para impedir que los datos de sus usuarios fueran accedidos y compartidos por un tercero en contravía de la normatividad de la compañía; además, Facebook ha reconocido vulnerabilidades en su plataforma que permitió a terceros hurtar "tokens" de acceso a Facebook, que luego podrían ser empleadas para tomar el control de cuentas de usuarios.
Decisión	Debido a que las medidas de seguridad de Facebook no son suficientes ni adecuadas para garantizar la seguridad de los datos de millones de personas; que la seguridad de la información es una condición crucial del tratamiento de datos personales por lo que se deben tomar acciones que garanticen la protección de estos.
	Conforme al principio y el deber de seguridad, así como el de accountability, la SIC impartió con carácter preventivo las órdenes que se desglosan aquí de manera resumida:
	● Facebook debe adoptar nuevas medidas, y robustecer las que ya tiene, para que sean apropiadas, útiles, eficaces y demostrables para cumplir con el deber de seguridad en la regulación colombiana.
	● Facebook debe desarrollar, implementar y mantener un programa integral de la seguridad de la información que garantice confidencialidad e integridad de los datos personales, manteniendo evaluaciones de los riesgos inherentes al tratamiento de la información.
	● Facebook deberá desarrollar, implementar y mantener las medidas necesarias para impedir el acceso por parte de terceros a los datos personales de los usuarios y a los de sus amigos sin su consentimiento, o a la información que no sea necesaria para el servicio adquirido por los usuarios; así mismo deberá modificar la configuración de privacidad, de tal manera que permita a los usuarios controlar la manera en cómo su información es compartida dentro de la aplicación y en las aplicaciones tercerizadas.
Decisión	● Facebook debe desarrollar medidas que garanticen la devolución o supresión de los datos personales, una vez finalizado el tratamiento de los mismos; además, deberá ajustar los contratos con los aliados comerciales para que el tratamiento de los datos cumpla con lo establecido en la ley 1581 del 2012.
	Para esto la SIC le dio un término de cuatro meses a Facebook en el cual debía demostrar el cumplimiento a través de una certificación emitida por una empresa independiente que acredite la implementación de las medidas ordenadas.

Elaboración propia. Información obtenida de la Resolución 1321 de 2019 de la Superintendencia de Industria y Comercio.

Con base en lo anterior, enviamos un derecho de petición a la SIC para conocer principalmente cuáles fueron las medidas adoptadas por Facebook para el cumplimiento de la Resolución 1321 de 2019. La petición fue la siguiente:

"PRIMERA: Solicito se me informe cuales fueron las medidas adoptadas por Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited para el cumplimiento de la Resolución 1321 de 2019.

SEGUNDA: Con base a lo anterior, solicito se me informe la efectividad de las medidas adoptadas por Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited.

TERCERA: Solicito se me informe del estado actual del cumplimiento de las órdenes emitidas por la Superintendencia de Industria y Comercio en la Resolución 1321 de 2019 en contra de Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited.

CUARTA: Solicito se me informe si la Superintendencia de Industria y Comercio ha tomado otro tipo de acción frente a Facebook Colombia SAS y lo que ahora se denominan los servicios de la plataforma META en el territorio nacional en concordancia con los vínculos jurídicos y económicos con las sociedades FACEBOOK GLOBAL HOLDING II, LLC y META PLATFORMS INC."

La respuesta de la entidad a la primera petición fue la siguiente:

"Sobre el particular le informamos que, la sociedad Facebook Inc., dando cumplimiento a lo ordenado en la Resolución 1321 de 2019, el 8 de mayo de 2020 remitió a está Superintendencia un reporte elaborado por el señor Jason N. Smolanoff, Director Gerente Senior y Líder Global de Prácticas de Seguridad Cibernética para Kroll, una compañía global de gestión de riesgos. Aquel documento fue objeto de análisis técnico y jurídico por parte de esta Dirección, concluyendo que con éste se dio cumplimiento a la Orden impartida.

Se aclara que no es posible suministrar información detallada respecto de las medidas adoptadas por dicha sociedad toda vez que, en la comunicación de 8 de mayo del 2020, citada líneas atrás, la empresa expresamente señaló que dichos documentos tienen el carácter de confidencial, en la medida que contiene información y datos que son de propiedad de esta, de tal manera que debemos dar aplicación a lo dispuesto por el artículo 61 del Código de Comercio". (Superintendencia de Industria y Comercio, 2023)

A la segunda y tercera petición, la entidad reiteró la misma respuesta. A la cuarta petición, la SIC respondió con la información de la Resolución 29826 del 19 de mayo de 2021 en donde se impartió una orden a la compañía Whatsapp Llc para que creara una política de tratamiento de la información que cumpliera con la normatividad colombiana. Dicho esto, es evidenciable como en Colombia hay una normatividad clara respecto de los parámetros que deben de seguir los operadores de datos, sumado a esto que la SIC ha realizado una labor dinámica por medio de la publicación de cartillas, documentos, y demás herramientas con el objetivo principal de que no se violen los derechos que abarca el habeas data de los titulares de los datos personales.

A pesar de lo anterior y en concordancia con la Resolución 1391 de 2019, cabe establecer que se pueden presentar desacatos a la normatividad colombiana en materia de datos personales, puesto que la aplicación de esta muchas veces es efectiva únicamente cuando se inician investigaciones. Debemos tener claridad en que hay una normatividad específica, donde los manuales son una herramienta fundamental para adherirse a los parámetros necesarios de la protección de datos personales. Están así mismo los canales de asesoría en la SIC para los responsables de tratamientos de datos personales y demás herramientas para que no se vulnere el derecho al habeas data; sin embargo, es responsabilidad de los operadores adherirse a la normatividad.

Por otra parte, se puede evidenciar como no se permite una veeduría ciudadana en el control de los operadores de datos personales, esto teniendo en cuenta que la SICordena a Facebook tomar medidas demostrables que garanticen la seguridad de las personas en referencia a los datos personales, pero estos no son demostrables a la ciudadanía porque el secreto industrial no lo permite.

Conforme al principio de accountability, del cual hablamos anteriormente, los responsables de datos personales deben suministrar una descripción de los procedimientos usados para la recolección de los datos personales y evidencia sobre la implementación efectiva de medidas de seguridad en las bases de datos; con certeza podemos decir que la descripción de las implementaciones que en este caso Facebook hizo en su base de datos, no comprometen el secreto industrial, puesto que no hay una revelación técnica o parametrizada del sistema que se implementó. En lo relativo al principio de accountability, hay una clara fricción entre la veeduría ciudadana para la protección de los datos personales y el secreto industrial, en el sentido en que nos encontramos ante operadores de datos, los cuales aparentan tener las medidas de seguridad necesarias, pero de las cuales la ciudadanía no tiene certeza alguna.

8. Conclusiones

El derecho al habeas data es un derecho constitucional, el cual garantiza la intimidad personal, el buen nombre, la información, la dignidad humana y entre otros. En donde ha tenido un desarrollo en el ordenamiento jurídico colombiano que establece unas disposiciones específicas para la protección de este derecho, pues garantiza que los datos personales que se registran en bases de datos tengan un manejo adecuado. Es decir que toda persona jurídica sin importar su naturaleza tiene la obligación legal de desarrollar bases de datos con una buena seguridad para la información de sus usuarios y darle aún más un trato especial toda información que puede ocasionarle un daño, como lo sería la discriminación.

En el caso de la aplicación de Facebook es una red social masiva, que constantemente recopila en sus bases de datos la información personal de millones de usuarios, como cualquier red social sin embargo lo que nos tenemos que enfocar es que en el caso de Facebook tiene que estar ligado a las normas de cada país en el cual presta su servicio, es decir que Facebook está ligado a las normas colombianas para operar en territorio colombiano, en donde se debe acoplar a la normativa nacional para la protección de datos personales.

La forma en como esta red social recopila la información en sus usuarios no se limita a la interacción con amigos, familias dentro de la misma red, sino que también puede recopilar información sin estar usándose, esto por medio de búsquedas en internet por decir alguno

No obstante Facebook asegura que recopila información de acuerdo con la normatividad de cada país, y que lo hace con el consentimiento de sus usuarios a través de la aceptación de términos y condiciones dentro de la aplicación. La información es recopilada en parte con la intención de personalizar y mejorar sus productos, y nos enfatiza que los datos personales no se venden.

El usuario al ser la parte débil de esta relación, se le a dado múltiples herramientas para su protección a la información, por parte de Facebook dándoles algunas como el cambio de contraseña o restringir a los usuarios, no obstante, este tipo de herramientas no garantizan una seguridad y tampoco dan una solución a largo plazo, es decir si un usuario es bloqueado por otro, simplemente puede llegar a crear otra cuenta y seguir hostigando.

Igualmente, la ley contempla algunos mecanismos para que el usuario no se quede sin recursos o protección, una sería el derecho de petición, la denuncia ante la SIC, o la última herramienta en caso de que aún se siga afectando el derecho fundamental del habeas data del usuario y es la acción de Tutela.

También se puede concluir que la SIC es la entidad pública con la función de proteger los datos personales de los usuarios, esto gracias a la ley estatutaria 1581 de 2012, en el cual esta entidad a estado expidiendo numerosas cartillas con el fin de promulgar una mejor protección a los datos personales, también el de poder sancionar y multar a las empresas si no cumple con los mínimos requisitos que impone la norma, esto se refleja en Facebook en la cual fue sancionada por no cumplir dichos parámetros.

Nosotros al tratar de saber en como resulto y el cómo se ha ido desarrollando esto entre Facebook y la SIC, interpusimos un derecho de petición en el cual la respuesta fue que, al ser secretos industriales, se reserva ese derecho. Frente a esta situación consideramos que no se nos está permitiendo tener una libre participación ciudadana en donde se limita, impidiendo saber el cómo se ha ido atendiendo el llamado de atención de la SIC

Facebook ha ido desarrollando medidas apropiadas para la privacidad de sus usuarios, por medio de su centro de privacidad, el cual se enfoca directamente en los datos de los usuarios y ofrece diversas opciones, pero una de las críticas que podemos contemplar es la dificultad que pude llegar a presentar el usuario al momento de utilizar dichas opciones, es decir no es una herramienta efectiva debido que no cualquier usuario la pueda ejercer.

Referencias Bibliográficas

ABC Internacional (17 de marzo de 2018) Una consultora que trabajó para Trump robó a Facebook datos de 50 millones de usuarios para influir en las elecciones. ABC Internacional. https://www.abc.es/internacional/abci-trump-robo-facebook-datos-50-millones-usuarios-para-influir-elecciones-201803172343_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Finternacional%2Fabci-trump-robo-facebook-datos-50-millones-usuarios-para-influir-elecciones-201803172343_noticia.html

Angarita, N. R. (2013). Tratamiento de datos personales Aproximación internacional y comentarios a la ley 1581 de 2012 . Bogota: Legis .

Burgués, C. (2018). Por qué roban las aplicaciones tus datos y para qué los utilizan. FAq-Mac. https://www.faq-mac.com/2018/09/por-que-roban-las-aplicaciones-tus-datos-y-para-que-los-utilizan/ Castañeda, L. (2010). Aprendizaje con redes sociales. Tejidos educativos para los nuevos entornos. Bogotá.

Constante. A. (2013). ¿Qué son las redes sociales? 01_A_Constane_Que_son_Redes_sociales_2013.pdf (unam.mx)

Constitución Política de Colombia [Const] Art 15 (7 de julio de 1991).

Corte Constitucional de Colombia, Sentencia C-748 de 2011. (M.P. Jorge Ignacio Pretelet Chaljub)

Corte Constitucional, Sentencia C-602-16, M.P. Alejandro Linares Cantillo. 2016.

Corte Constitucional, Sentencia T-509-20, M.P. José Fernando Reyes Cuartas. 2020.

Corte Constitucional, Sentencia T-114-18, M.P. Carlos Bernal Pulido. 2018.

Decreto 1377 de 2013 [presidente de la República de Colombia] Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. 27 de Junio de 2013.

Gomez, C. C. (2022). 'ACCOUNTABILITY' Y CARGAS PROBATORIAS EN EL TRATAMIENTO DE DATOS PERSONALES. legis.https://xperta.legis.co/visor/rmercantil/rmercantil_bf-1da44b847fc5c406f96412df14fca0ef0nf9/revista-foro-de-derecho-mercantil/%e2%80%98accountability%e2%80%99-y-cargas-probatorias-en-el-tratamiento-de-datos-personales

https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf.

Ley 1266 de 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. 31 de diciembre de 2008. D.O. No. 47.219.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 18 de octubre de 2012. D.O. No. 48.587. LEY 1712 DE 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 06 de marzo de 2014. D.O. No. 49.084.

Ley 1755 de 2015. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. 30 de junio de 2015. D.O. No. 49.559.

López, J. Peiró, R. (2021). Tipos de información. Tipos de información - Qué es, definición y concepto. Economipedia. https://economipedia.com/definiciones/tipos-de-informacion.html.

Marquez, D. (2020). ¿Cómo las APP roban información y qué hacen con ella después?. Tekcrispy. https://www.tekcrispy.com/2020/08/03/apps-roban-informacion/#:~:text=%C2%BFC%C3%B3mo%20las%20aplicaciones%20obtienen%20nuestra%20informaci%C3%B3n%3F%201%20Los,...%203%20Aplicaciones%20falsas%20y%20trampas%20reales%20

Meta (2022) Condiciones del Servicio, Condiciones que aceptas al usar Facebook https://www.facebook.com/legal/terms.

Meta (S.F) ¿En qué consiste el Reglamento General de Protección de Datos (RGPD)? https://www.facebook.com/business/gdpr.

Meta (S.F) Centro de Privacidad https://www.facebook.com/privacy/center/?entry_point=facebook_settings.

Meta (S.F) Centro de Trasparencia https://transparency.fb.com/data/.

Meta (S.F) Herramientas y políticas de seguridad https://about.meta.com/actions/safety/topics/safety-basics/tools/

Meta (S.F) Política de privacidad ¿Qué es la Política de privacidad y qué cubre? https://www.facebook.com/privacy/policy.

Peña, N. (2017). Contratos empresariales nacionales e internacionales. https://app-vlex-com.sibulgem.unilibre.edu.co/##sources/24770/chapter:64685129

Roa, M. A. (2013). "FACEBOOK FRENTE AL DERECHO A LA VIDA PRIVADA Y LA PROTECCIÓN DE DATOS PERSONALES". Santiago de Chile: UNIVERSIDAD DE CHILE.'

Rodriguez, C. (2021). Las formas discursivas y la protección de datos personales en las redes sociales Facebook Inc. Buenos Aires: Universidad de San Andrés.

Rojas, M. (2014). EVOLUCIÓN DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA RESPECTO A ESTÁNDARES INTERNACIONALES. Novum Jus: revista especializada en sociología jurídica y política, 107-109.

Roncancio., A. M. (2019). Protección del derecho de Habeas Data en plataformas virtuales. Boletín Colegio de Abogados Comercialistas, 15-16.

Santos, E. (2010). REDES SOCIALES: TEJIENDO DATOS PERSONALES POR LA WEB. REVISTA FORO DERECHO MERCANTIL N°:28, 53-95.

Sotelo, D. A. (2012). EL HABEAS DATA EN LAS REDES SOCIALES ONLINE: RESPONSABILIDAD Y VIGILANCIA. REVISTA ITER AD VERITATEM Nº. 10, 231-250.

Superintendencia De Industria Y Comercio (S.F) Denuncias y Demandas en Materia de Protección al Consumidor https://www.sic.gov.co/denuncias-y-demandas-en-materia-de-proteccion-al-consumidor

Superintendencia De Industria Y Comercio, (2023) Respuesta a la solicitud bajo números 23-00000-000 y 23-164398. Trámite 317 de actuación 440.

Superintendencia De Industria Y Comercio, Resolución N 1321 De 2019

Superintendencia De Industria Y Comercio, Resolución N 21478 De 2019

Superintendencia De Industria Y Comercio. (2016), Guía Para La Implementación Del Principio De Responsabilidad Demostrada (Accountability) , https://issuu.com/quioscosic/docs/guia_accountability_26_p__g

Superintendencia De Industria Y Comercio. (2017), Formato modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios

Superintendencia De Industria Y Comercio. (2019) Guía para la implementación del principio de responsabilidad demostrada.

Superintendencia De Industria Y Comercio. Página Oficial https://www.sic.gov.co/

Vélez, A. V. (2021). El ámbito de aplicación del régimen jurídico colombiano para la protección de datos personales. Su alcance frente a empresas extranjeras sin representación jurídica en en Colombia. Bogotá.