RESUMEN – TRABAJO DE GRADO

AUTORES	Herbert Iván Díaz Torrado Código: 250741 Javier Andrés Bayona Navarro Código: 250743		
FACULTAD	**Facultad de educación, artes y humanidades**		
PLAN DE ESTUDIOS	**Derecho**		
DIRECTOR	Robinson David Verjel Ropero		
TÍTULO DE LA TESIS	**La utopía de la protección de datos personales en las redes sociales en Colombia**		
TITULO EN INGLES	The utopia of the protection of personal data in social networks in Colombia		

RESUMEN
(70 palabras)

Tras analizar esta situación jurídica, se pudo determinar que en Colombia si resulta utópica la protección de los datos personales a través de las redes sociales, por cuanto el mismo sistema normativo y jurisprudencial desconoce la necesidad de regular el uso y manejo de las redes sociales; adicionalmente, en materia de responsabilidad de los operadores la jurisprudencia aún se encuentra en discrepancias sobre la imputación o no de esta.

RESUMEN EN INGLES

After analyzing this legal situation, it was possible to determine that in Colombia the protection of personal data through social networks is utopian, since the same regulatory and jurisprudential system ignores the need to regulate the use and management of social networks; additionally, in terms of operator liability, the jurisprudence is still in discrepancies on the attribution or not of this.

PALABRAS CLAVES	Datos personales, redes sociales, responsabilidad de medios y de resultados
PALABRAS CLAVES EN INGLES	Personal data, social networks, media and results responsibility

CARACTERÍSTICAS			
PÁGINAS: 43	PLANOS:	ILUSTRACIONES:	CD-ROM:

La utopía de la protección de datos personales en las redes sociales en Colombia

Autores

Herbert Iván Díaz Torrado Código: 250741

Javier Andrés Bayona Navarro Código: 250743

Facultad de educación, artes y humanidades, Universidad Francisco de Paula Santander Ocaña,

Programa de Derecho

Robinson David Verjel Ropero

Abogado

18 de abril del 2022

Indice

Capitulo. El tratamiento normativo y jurisprudencial de los datos personales en Colombia 5

1.1 Espectro internacional de los datos personales 5

1.2 Los datos personales en el estado social de derecho.....11

1.3 Mecanismos legales de protección.....12

1.4 Visión jurisprudencial.....15

Capítulo 2. Inexistencia de regulación de redes sociales en Colombia.....18

2.1 Doctrina sobre las redes sociales 18

2.1.1 Las redes sociales 18

2.1.2 Principales redes sociales.....19

2.2 Situación jurídica en Colombia.....20

2.3 Modelo de regulación de redes sociales.....25

Capítulo 3. Responsabilidad de medios por parte de las operadoras de redes sociales y sus efectos jurídicos 27

3.1 Naturaleza de la responsabilidad de medios 27

3.1.1 Distinción entre obligaciones de medios y obligaciones de resultados.....27

3.1.2 Las obligaciones de medios de las operadoras de redes sociales 28

Capítulo 4. La culpa grave en las empresas operadores de redes sociales y sus efectos jurídicos en Colombia.....33

4.1 Estadios de la Culpa.....33

4.2 Efectos jurídicos de la culpa grave 34

Conclusiones.....36

Referencias.....38

Introducción

En Colombia, la protección de datos personales y el régimen normativo de dicha disposición, surge en el marco de la Constitución Política de 1991, donde se reconoce que la recogida, sistema y distribución de los archivos, se respetarán otras libertades garantizadas previstas en la Carta Magna. (Const, Art. 15)

Con el alto crecimiento de las Tecnologías de la Información y la comunicación, se comienza a generar una regularización sobre la circulación de los datos personales en medio de estos dispositivos móviles.

En el marco de esta obligación estatal, se expide la Ley estatutaria 1266 de 2008 donde se establecen avances importantes en materia legal, sobre los derechos básicos para la protección del habeas data.

Con la promulgación de la Ley 1581 de 2012, se establecieron nuevos avances, en lo que respecta al amparo de los datos que son administrados por entidades públicas y privadas, regulándose lo relacionado con los datos sensibles y los datos personales de niños y jóvenes.

En el mismo contexto, se han expedido otro conjunto de normas relacionadas con la seguridad en la web, así como en lo referente a la reserva y las TIC.

Referente al tratamiento de datos personales, la ley colombiana se fundamenta en la exclusividad del titular de los datos, y en caso del uso de estos, se deberá acreditar la

autorización del propietario, siendo requisito esencial la autorización que deberá informar al titular de los datos e indicar la finalidad del tratamiento.

Sin embargo, la realidad palpable en redes sociales permite evidenciar, que en el solo registro en la plataforma, el usuario está haciendo click y aceptando las condiciones que bien se podrían definir como un contrato solemne, en el cual además se entrega la información personal, para que pueda ser compartida. No obstante, encontramos números escándalos de videos íntimos y demás, que han sido subidos a dichas plataformas, y que han victimizado, discriminado, vulnerado y demás a los protagonistas, su vínculo familiar y demás, a través de la exposición de información privada, que se roto en plataformas digitales.

Frente a ello, surge un debate en relación la utopía de la protección de datos personales en redes sociales en Colombia. Se presentarán cuatro capítulos, el primero de ellos enfocado en el análisis de la protección de datos en Colombia, el segundo sobre la inexistencia de regulación de redes sociales en Colombia, el tercero con un enfoque hacia la responsabilidad de medios de los operadores de redes sociales y finalmente el último capítulo plantea la culpa grave por captación o perdida de datos personales por parte de los operadores de redes sociales y sus efectos jurídicos.

El desarrollo de la investigación jurídica, se elaborará bajo el enfoque exegético, que permite desglosar las motivaciones o argumentos del legislador al instante de invocar la regla normativa.

Capitulo. El tratamiento normativo y jurisprudencial de los datos personales en Colombia

1.1 Espectro internacional de los datos personales

En el espectro internacional, la protección de los datos personales se encuentra enmarcada en los diferentes instrumentos jurídicos expedidos por organizaciones como la Organización de las Naciones Unidas, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión y las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.

Desde la óptica de la organización para la Cooperación y el Desarrollo Económico (en adelante OCDE) se han establecido algunas recomendaciones a partir de 1980 relacionadas directamente con la protección de la intimidad y la circulación transfronteriza de datos personales. Dentro de dicha herramientas establecen algunas reglas que busca brindar a los ciudadanos garantías en materia de protección a los derechos individuales que se ven inmersos en los procesos de transferencias de datos, así como promover la democracia, el respeto por los derechos humanos y la economía de libre mercado.

A través de dicha herramienta jurídica se promueven principios como:

1. Principio de limitación de la recogida
2. Principio de calidad de los datos
3. Principio de especificación de la finalidad
4. Principio de limitación de uso

5. Principio de salvaguardas de seguridad
6. Principio de apertura de los datos
7. Principio de participación individual
8. Principio de responsabilidad

En línea con lo anterior, también a través de la OCDE se han promovido otras directrices en la que se busca salvaguardar la trasferencia de datos personas, a través de parámetros como transparencia pública y acceso a la información, privacidad en redes globales y comunicaciones electrónicas no solicitadas.

Dichas herramientas desde el espectro de dicha organización solo funcionan como herramientas de guía, pues su naturaleza jurídica impide un carácter vinculante en los Estados, es decir que no son parámetros obligatorios para implementar dentro de cada régimen jurídico.

En seguimiento a estos instrumentos internacionales se encuentra que la Asia Pacific Economic Cooperation (APEC) Privacy Framework, donde constantemente se tratan temas relacionados con el intercambio comercial, coordinación y cooperación entre las economías de diferentes países, en el año 2004 expidió un Marco de Privacidad donde es busca fortalecer la protección de la privacidad y permitir los intercambios de información.

A través de dicho documento se enfatiza en la necesidad de regular y controlar a las entidades encargadas del tratamiento de datos, así como de la revisión de la intervención de las autoridades públicas en este contexto, por la responsabilidad en la optimización de la economía.

De ambas herramientas jurídicas internacionales, Colombia ha adoptado algunas medidas encontradas en la Ley 1581 de 2012, como son los principios de prevención del daño, donde el legislador prevé acerca de las malas prácticas o uso indebido de la información recolectada y el daño causado a los titulares de la información.

A través de la Comunidad Iberoamericana también se han promovido directrices, como son las expedidas por la Red Iberoamericana de Protección de Datos, como resultado de un acuerdo entre varios países en el año 2003 en Guatemala. A través de dicho documento, se establecen algunos lineamientos direccionados con el derecho al habeas data reconocida como un derecho fundamental y autónomo frente al derecho a la intimidad. Las recomendaciones establecidas en este instrumento se encuentran direccionadas con la protección a través de un conjunto de principios, derechos y deberes, logrando que se establezca un marco homogéneo de protección que facilite el intercambio de información entre ellos y hacia otros Estados que han adoptado estándares equivalentes o similares de protección.

Los principales lineamientos establecidos por la Red Iberoamericana de Protección de Datos, se enmarcan en un tratamiento leal y lícito, es decir, que la información recolectada sea tratada bajo el principio de la buena fe, y con observancia de las disposiciones legales y las disposiciones que se han implementado para la protección de los derechos de las personas; asi mismo se plantea la limitación de la finalidad, es decir que se deberá dar claridad sobre el objeto del tratamiento de la información recolectada; en el mismo sentido, se plantea la proporcionalidad, es decir que debe existir una equivalencia entre el tratamiento y los datos recolectados; exactitud, que se refiere a que los datos se mantengan exactos, completos y

actualizados y finalmente conservación que hace referencia a que los datos se cancelen o se conviertan en anónimos cuando hayan dejado de ser necesarios para las finalidades que se previeron. (Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, 2006)

A través de estas directrices se establece un concepto de legitimación para el tratamiento, donde se dispone que los datos puedan ser recabados o tratados cuando se obtengan con el consentimiento del interesado, o si una norma interna lo establece a través de excepciones razonables y legítimas.

A la par de este concepto, se reconocen como derechos del titular de los datos personales, el acceso, la rectificación, la cancelación, la oposición al tratamiento, la indemnización por daños sufridos como consecuencia de un tratamiento de datos que haya contrariado las directrices, entre otros.

Adicionalmente, se establece como prioridad la seguridad y la confidencialidad en el tratamiento de datos personales, razón por la cual es deber de cada Estado establecer medidas para la protección de datos contra la adulteración, pérdida, acceso no autorizado o uso fraudulento.

Referente a la transferencia de datos a nivel internacional, se habla en estas directrices de algunas limitaciones o reglas como que solo se podrán efectuar las transferencias de datos entre los Estados que tenían una legislación interna que recoja lo dispuesto en este documento.

Finalmente, a través de las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana se prevé de la importancia de que cada Estado regule internamente lo relacionado con el tratamiento de datos y que se impongan sanciones cuando se vulnere dicho régimen a través de las autoridades judiciales, por lo que se establece en la regulación de este tema que se acuda a la vía judicial para que se garantice el cumplimiento de dichos parámetros. (Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, 2006)

Por su parte, en la Organización de Naciones Unidas (ONU) hacia el año 1990 se expidió la Resolución 45/95 donde se reglamentan un conjunto de principios para la protección de datos personales en el entorno internacional. Dichos principios se enmarcan en el principio de licitud y lealtad, donde la información no podrá tratarse con procedimientos ilegales, o usarse para fines contrarios a las disposiciones de la Carta de Naciones Unidas; el principio de exactitud que plantea la verificación y veracidad de la información recolectada; el principio de finalidad, que busca que los datos recolectados sean con un fin y un objetivo específico; el principio de acceso de la persona interesada, el principio de no discriminación, es decir que no no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, obre la participación en una asociación o la afiliación a un sindicato; la facultad de establecer excepciones, es decir, que solo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás.

En el mismo sentido, se ha planteado el principio de seguridad Se deben adoptar medidas apropiadas para proteger los ficheros contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático; el de control y sanciones, donde se consagra que dentro de cada legislación debe designar a la autoridad que, de conformidad con el sistema jurídico interno, se encarga de controlar el respeto de los principios anteriormente enunciados y finalmente el principio de Flujo de datos a través de las fronteras, que implica que cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos.

Mediante el Consejo de Europa se expidió en el que se establecen algunos criterios sobre el tratamiento de datos personales en el sector público y privado. En el artículo 12 se dispone que:

"Flujos transfronterizos de datos de carácter personal y el derecho interno

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.
2. Parte no podrá con el fin de proteger la vida privada prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. .

A través de este importante instrumento internacional se amplió el conjunto de garantías prescritas para la protección de datos, específicamente en lo que se refiere a los datos sensibles, es decir, aquellos que revelan de la persona aspectos como su vida sexual, opiniones políticas, entre otros.

Por su parte el Parlamento Europeo promulgó la Directiva 95 N° 95/46/CE en la que hace referencia al tratamiento de datos personales y la libre circulación de dichos datos, regulándose de manera exhaustiva algunos criterios. Al respecto, el artículo 1 dispuso que:

> "Los Estados miembros garantizar con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad en lo que respecta al tratamiento de los datos personales."

Bajo estas disposiciones en el escenario internacional, se puede coludir que las diferentes organizaciones y estamentos en este espectro han compilado un conjunto de criterios claros sobre la protección de los datos personales y la responsabilidad de los Estados en establecer criterios jurídicos para la limitación en la circulación de los mismos bajo una serie de principios, y la recomendación de legislar en la materia, lo que supone una gran preocupación e importancia de dichas entidades para brindar a los ciudadanos un marco de mecanismos jurídicos para la protección de sus datos personales.

1.2 Los datos personales en el estado social de derecho

La transformación del Estado de derecho al Estado Social de derecho previsto por la Constitución Política de 1991, trajo consigo la expedición de un catálogo de derechos fundamentales, donde se prevé la protección de los datos personales del ciudadano. En la trascripción que se hace del artículo 15 de la Constitución Política de Colombia, se establece la protección al derecho a la intimidad personal y familiar, así como al buen nombre. En el mismo contenido jurídico, se hace énfasis en la protección de los datos personales a partir del derecho que gozan los ciudadanos para conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (Const, Art. 15)

Bajo este precepto constitucional, se reconoce entonces el desarrollo del derecho a la intimidad, buen nombre y protección de datos en el marco del Estado Social de derecho, y que tiene como finalidad equilibrar las relaciones entre los titulares de los datos y las entidades del sector público o privado que realizan el tratamiento de estos. De esta manera, la disposición de la Constitución Política reconoce en la esfera de los derechos fundamentales la protección frente a la información suministrada y almacenada por los bancos de datos.

1.3 Mecanismos legales de protección

En Colombia la protección de los datos personales ha sido desarrollada a través de diferentes normas que buscan materializar el mandato del artículo 15 de la Constitución Política. Bajo este precepto el primer antecedente para la unificación de criterios en materia de protección de datos personales fue precedido por la Honorable Corte Constitucional a través de la Sentencia T-729 de 2002, donde se establecieron los principios mínimos de protección de datos personales.

A Partir de dichos criterios jurisprudenciales se fijaron como principios de protección a los datos personales en Colombia, el principio a la libertad, que consiste en el conocimiento previo del titular de los datos personales para su tratamiento; el principio de necesidad que abarca que los datos recolectados serán aquellos necesarios para el objeto perseguido, concretándose así que no se puede registrar o circular aquella información que no sea necesaria; el principio de integridad, que confía la necesidad de verificar la autenticidad de los datos suministrados; el principio de integridad va de la mano del anterior, en el que el registro de los datos personales deberá ser parcial, completo e integral; principio de finalidad, que comprende la necesidad de que se persiga un fin o necesidad; el principio de utilidad, es decir que los datos recolectados deberá cumplir una finalidad determinada; el principio de circulación restringida, donde se establecen una serie de limitaciones para su circulación; el principio de incorporación que opera para el titular cuando le conviene incluir información adicional y las entidades no se podrán negar a estas peticiones; principio de caducidad en el que se establece que no se podrán recolectar estos datos para contenerlos de forma indefinida; principio de diligencia en el manejo de los datos personales y el principio de la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración, deviene cuando se presentan fallas en el proceso y se configuren los elementos generales de la responsabilidad civil, imponiéndosele la carga a titular de la información de demostrar que el daño sufrido fue a causa de la actuación del operador de los datos". (Corte Constitucional, 2002, Sentencia T-729)

Sin embargo, fue bajo la promulgación de la Ley 1226 de 2008 donde por primera vez el legislador se aproximó a la protección de datos personales, a través del desarrollo de la figura del Habeas Data, y que se encuentra encaminada a la salvaguarda de la información recolectada y las

obligaciones dinerarias que se establece con entidades financieras, comerciales, crediticias o de servicios, por lo cual el legislador vio la necesidad de crear una legislación especial y diferenciada a la aquí mencionada que propendiera por la protección de datos personales que se encontraran por fuera del ámbito objeto de la Ley de habeas data.

No obstante, la misma Corte Constitucional a través de la Sentencia C-1011 de 2008 se advirtió que la norma establecía una regulación parcial, todas vez que los argumentos planteados a través del proyecto de ley, tenía como fin la fijación de reglas para la administración de datos de contenido financiero y crediticio, por cuanto no es considerada por el Alto Tribunal como una norma integral que desarrolle ampliamente el derecho al Habeas Data. (Corte Constitucional, Sentencia C-1011 de 2008)

Bajo estas circunstancias, el legislador en el año 2012 expidió la Ley Estatutaria 1581 donde formalmente se establecen unos parámetros de protección a los datos personales de cara al derecho a la intimidad del titular, ante la carencia de mecanismos legales para tal fin.

En síntesis la norma recoge los siguientes lineamientos, donde los datos personales deben ser:

a) recogidos para los fines determinados, los cuales deberán ser explícitos y legítimos y no ser tratados posteriormente de manera incompatible con dichos fines,

b) adecuados, pertinentes, y no excesivos en relación con los fines para los cuales fueron recogidos,

c) exactos y actualizados y

d) conservados de forma en que se permita la identificación de los interesados durante el periodo requerido para los fines recolectados

Bajo este marco de protección jurídica se establece como categoría especial los datos sensibles y los datos personales de los niños, niñas y adolescentes, por cuanto en ellos se ve incurso el derecho a la intimidad y su uso indebido puede generar vulneración en aspectos personales como la vida sexual, ideales políticos, entre otros. En materia de datos de los menores de edad, el tratamiento de estos busca la plena protección de los derechos fundamentales del menor y con miras a la "realización del principio de su interés superior".

Dicha disposición normativa entró en vigencia a partir del año 2013, exigiéndose a los encargados del tratamiento de datos la elaboración de una manual con las condiciones de protección de datos personales, para conocimiento del personal y del titular de la información. Adicionalmente, se expidió el Decreto 1377 de 2013 como complemento de la Ley 158, donde se reglamentó aspectos como la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros .

1.4 Visión jurisprudencial

En el escenario jurisprudencial, la Corte Constitucional ha venido emitiendo algunos criterios en materia del tratamiento de los datos personales en el entorno jurídico colombiano, tal como los principios descritos en la Sentencia 414 de 1992 donde se puntualiza en la necesidad de

garantizar el derecho a la intimidad, por lo que la protección de datos se debe dar en la esfera privada y familiar, y no puede intervenir ni el Estado ni otros particulares.

Siguiendo esta línea jurisprudencial, se emitió la Sentencia SU-082 de 1995 donde dentro de marco del derecho a la autodeterminación informática y a la libertad económica se configuran como el de conocer la información que haga referencia al titular de los datos, el derecho a la actualización de dicha información y finalmente a la rectificación de la información que no corresponda a la verdad y a la caducidad del dato negativo en las bases de datos. (Corte Constitucional, 1995,Sentencia SU-082)

En providencia del año 2002, la Corte Constitucional realizó una diferenciación entre el habeas data y el derecho al buen nombre y a la intimidad, en situaciones como la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información. (Corte Constitucional, 2002, Sentencia T-729)

Más adelante, como se mencionó anteriormente en Sentencia de Constitucionalidad 1011 de 2008 se estableció que el derecho al Habeas Data configura la facultad del titular de los datos, a un conjunto de libertades para contra la información de sí mismo que fue recopilada por un banco de datos, por lo que se deberán preservar los intereses de este ante el posible abuso de poder informativo. A través de esta providencia se reconocen derechos como el conocimiento y acceso a la información recolectada en las bases de datos; el derecho a la inclusión de nuevos

datos, el derecho a la actualización de la información, y el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad. (Corte Constitucional, Sentencia C-1011 de 2008)

Finalmente, expresa la Corte Constitucional, a través de esta providencia el reconocimiento del que gozan los titulares de los datos personales, al a que excluya la información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular —salvo las excepciones previstas en la normativa. (Corte Constitucional, Sentencia C-1011 de 2008)

Capítulo 2. Inexistencia de regulación de redes sociales en Colombia

2.1 Doctrina sobre las redes sociales

2.1.1 Las redes sociales

Las tecnologías de la información y la comunicación han causado un verdadero impacto en los seres humanos durante las últimas dos décadas. Dentro de los grandes beneficios que ha traído esta tecnología, se encuentra la facilidad para comunicarse los seres humanos, desde diferentes plataformas y las modalidades para desarrollar actividades laborales, académicas, sociales y de entretenimiento.

Sobre esta última fase se encuentran las redes sociales que comienzan su proceso de surgimiento desde el año 2000 y 2002 cuando se lanza el portal Friendster, que alcanza los tres millones de usuarios en solo tres meses.

Hacia el año 2003 se da vida a las redes MySpace, LinkedIn y Facebook, aunque la fecha de esta última no está clara, puesto que llevaba gestándose varios años. Facebook fue creada por Mark Zuckerberg. Con la aparición de Facebook, vivieron redes como Hi5 y Netlog, Digg, como portal de noticias sociales; Bebo, con el acrónimo de “Blog Early, Blog Often”; y Orkut, gestionada por Google. 2005.

Más adelante se siguen gestionando Youtube, luego Twitter, Badoo. Pinterest. LinkedIn, WhatsApp e Instagram. Sin embargo, sobre todas ellas, Facebook ha sido la plataforma con más usuarios en todo el mundo.

Las redes sociales se han conceptuado desde diferentes órbitas de estudio, como sitios en la web donde sus usuarios publican y comparten información de tipo personal, profesiones, con terceras personas, algunos de su círculo y otros desconocidos. (Celaya, 2008)

El acceso a dichas plataformas digitales implica que los usuarios acepten términos y condiciones para el tratamiento de su información personal, profesional o social, poniéndose en manos de los operadores de las redes sociales, quienes a través de dicho contrato se inhiben de responder por los perjuicios ocasionados en el ámbito material e inmaterial, ante la exposición de datos personales en dichas plataformas digitales.

2.1.2 Principales redes sociales

Hoy por hoy las redes sociales como se anunció anteriormente ocupan un gran espacio dentro de las actividades que realizan los seres humanos desde la comunicación y el entretenimiento. Las más usadas en todo el mundo y sus principales funciones son:

Facebook: es una plataforma digital en la que los usuarios pueden reencontrarse con amigos de la infancia, liderar grupos de usuarios y ofrecer opciones de crear diversos grupos, compartir información personal, como fotos, videos, chats, entre otros.

Twitter: a través de esta plataforma digital se puede interactuar mediante mensajes con un límite de caracteres. Su reconocido hashtag se ha convertido en parte del lenguaje popular y es muy utilizado por las grandes empresas para promocionar sus productos.

Instagram: es una plataforma digital en la que los usuarios pueden acceder a servicios de publicación de fotos y videos, hacer uso de filtros, y demás herramientas para la edición de fotos y videos y compartir información personal a través de historias que duran 24 horas en línea y chats con otros usuarios.

Youtube: a través de esta reconocida plataforma se ha permitido a sus usuarios la publicación de videos. Con posterioridad, se desarrolló la posibilidad de transmitir videos en vivo y en directo, esta potente herramienta permite comunicar a personas de todas partes del mundo y resulta muy beneficiosa para artistas ignotos que desean hacerse a un lugar en la industria.

Myspace: Se trata de un portal especialmente usado por cantantes que buscan alcanzar la fama, es posible compartir música, videos y fotos, conocer a otros artistas y mantenerse en contacto con ellos e incluso crear blogs. (Congreso de la Republica de Colombia, Proyecto de Ley para regular las políticas de uso y apropiación de las redes sociales y se dictan otras disposiciones generales)

2.2 Situación jurídica en Colombia

En Colombia el tratamiento jurídico asignado al uso y manejo de las redes sociales se encuentra bastante alejado de un compendio normativo completo que les permita a los ciudadanos una protección completa en esta materia.

No obstante existen algunas disposiciones normativas en lo que se refiere a los delitos informáticos, castigados a través de la Ley 1273 de 2009, donde se establece el marco de protección a la información y a los datos en Colombia, y que aplica a aquellas conductas donde se configuran daños informáticos, captación de información personal y privada, usada para fines de extorsión, hurto y demás.

En el mismo escenario, también se contraen acciones para la protección de datos personales a través de la Ley 1581 de 2012 conocida como la Ley de Habeas Data, pero que no aplica para los datos contenidos en redes sociales como Facebook y Twitter, y tampoco de cualquier otra red social.

Sin embargo, en materia penal conductas punitivas como la injuria y la calumnia si son castigadas cuando se cometen a través de cualquier medio, incluido las redes sociales, sancionándose con medidas como la prisión de entre uno y tres años, y multas desde diez a mil salarios mínimos mensuales legales vigentes por el delito de injuria, y por la conducta de calumnia podrá incurrir en prisión de uno (1) a cuatro (4) años y multa de diez (10) a mil (1.000) salarios mínimos legales mensuales vigentes según el código penal colombiano. (Congreso de Colombia, Ley 599 del 2000)

No obstante, dichas disposiciones no son las respuestas que atienda en mayor proporción a las situaciones que se evidencian en redes sociales de manera constante, por cuanto si bien permiten al usuario algunos mecanismos de defensa de sus derechos, el alcance de la libertad de expresión en las plataformas digitales, las políticas de uso y privacidad de las mismas, la

ausencia de regulación y la falta de criterios para legitimar la responsabilidad de los intermediarios digitales, pone en una condición de vulnerabilidad o desventaja a los usuarios señalados, violentados, cercenados, humillados y perseguidos a través de alguna publicación en dichas plataformas digitales. Es decir, la injuria y la calumnia en redes sociales no atienden a las verdaderas necesidades cuando se ve en curso de una vulneración derechos fundamentales como la intimidad, el buen nombre o la imagen personal.

Otra conducta punitiva muy común en las redes sociales es el ciberacoso, razón por la cual el legislador a través de la expedición de la Ley 1620 de 2013, que permitió la creación del sistema nacional de convivencia escolar, estableciéndose límites en materia educativa para quienes a través de redes sociales realicen matoneo, imponiéndose sanciones que van hasta la expulsión de la institución educativa. Dentro de la misma política del Estado para estos casos se configuró la página web teprotejo.org que le permite a la Policía Nacional de Colombia conocer las denuncias virtuales por ciberacoso, contenidos ilegales en las plataformas digitales que ponga en riesgo a los niños, niñas y adolescentes, y con posterioridad a la denuncia se comienza el proceso de investigación, por lo que de hallarse un riesgo para esta comunidad, entonces se procederá al bloqueo de la URL.

El sexting es otra conducta común y peligrosa en las plataformas digitales y tiene desarrollo cuando se postean fotos o videos con contenido sexual y se comienza a compartir por este tipo de medios. El sexting se puede dar a través de diferentes situaciones y puede derivar en sextorsión que dentro del régimen jurídico colombiano es castigado mediante el artículo 244 del Código Penal modificado a través de la Ley 733 del 2002, donde se establece una sanción de

entre doce a dieciséis años de prisión y multa por la comisión de esta conducta. (Congreso de Colombia, Ley 733 del 2002)

Adicionalmente, conductas como la pornografía infantil que también es difundida a través de redes sociales se encuentra castigada en el régimen interno a través de la Ley 1336 de 2009 sancionando con prisión de diez (10) a veinte (20) años y multa de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes. (Congreso de Colombia, Ley 1336 de 2009)

Otro espectro donde se ven inmersas las redes sociales son los derechos de autor, protegidos en Colombia desde dos vertientes como son la propiedad industrial y el derecho de autor, a través de las normas adoptadas mediante convenios, acuerdos y tratados expedidos por la Organización Mundial de la Propiedad Intelectual, y por las disposiciones de la Carta Política en el artículo 61, donde se establece que " El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley". (Constitución Política de Colombia, 1991, Art. 61)

Penalmente, la infracción de estos derechos se encuentra contemplada en el Código Penal sancionándose con prisión desde treinta y dos meses hasta noventa meses. En plataformas digitales como Facebook y Twitter se protege este tipo de delitos mediante la promulgación de su política de uso donde se exige la originalidad de los contenidos cargados, por lo que se imputa la responsabilidad únicamente al usuario de lo que publica. Cuando un usuario crea un perfil en cualquiera de estas dos redes sociales debe leer bien las condiciones del servicio y políticas de

uso, porque al darle aceptar se le está otorgando a facebook y twitter toda facultad sobre la obra dentro de las cuales la puede almacenar, exhibir y realizar cualquier acto que le pueda convenir.

Dentro de la política de uso que han establecido plataformas como Facebook y Twitter se encuentra la existencia de una cláusula de exclusión de responsabilidad como intermediarios por los contenidos que sus usuarios suben a la red, recayendo la responsabilidad sobre estos últimos. Es preciso concluir que el avance abismal de las redes sociales, hace casi imposible que el derecho pueda alcanzar sus esferas, por lo que en razón de la regulación de mecanismos determinados para tales fines, Colombia se encuentra desprovisto de los mismos, por lo que actualmente lo que se hace es adecuar las conductas concebidas por el legislador penalmente y civilmente, para imputar responsabilidad y aplicar las debidas sanciones.

No obstante en materia del uso, control, restricciones y demás, siguen siendo los intermediarios digitales y dueños de las redes sociales quienes siguen imponiendo la mayoría de reglas, hacia sus políticas de uso seguridad, encontrándose el usuario seriamente en un estado de desventaja frente a la capacidad que tienen las redes sociales para atentar contra los derechos fundamentales de los usuarios, y en cuestión de minutos lapidar proyectos personales, laborales y profesionales.

Finalmente, durante los últimos cinco años, se han venido gestionando algunos proyectos de ley que ha buscado la regulación de estos medios de comunicación y entretenimiento, como el proyecto de ley presentado por José David Name Cardozo, y donde se incluyó como medios de información y denuncia la creación de una línea telefónica y una página electrónica para la

realización de las respectivas denuncias contra conductas lesivas o ilícitas publicadas en las redes sociales y señalar las páginas electrónica; así como, señalar a los autores o responsables de tales publicaciones.

En el mismo escenario planteaba el proyecto de ley, la imposición de sanciones administrativas para usuarios y administradores de las redes sociales como

1- Multas hasta de 100 salarios mínimos mensuales legales vigentes.

2- Cancelación o suspensión de la correspondiente página electrónica o perfil en las plataformas. (Congreso de la Republica de Colombia, Proyecto de Ley para regular las políticas de uso y apropiación de las redes sociales y se dictan otras disposiciones generales)

2.3 Modelo de regulación de redes sociales

Para efectos de la monografía es importante analizar cómo se ha regulado las redes sociales en el espectro internacional. El primer modelo se encuentra enmarcado en el Derecho que regula la Comunidad Europea donde mantienen una tendencia conservadora a través de un sistema positivo. En materia de redes sociales no se cuenta una regulación exclusiva, sino que da aplicabilidad al derecho comunitario europeo y se aplican normas del Derecho derivado, complementario y convencional para su uso, básicamente en aspectos como la protección de datos personales y el derecho fundamental a la intimidad.

Sin embargo, es relevante hacer mención de que la Comisión Europea suscribió el Código de Conducta con Facebook, Youtube y Microsoft, donde estas empresas se compromete

a implementar mecanismos y procedimiento para la eliminación de expresiones ilegales que promuevan el odio en dichas plataformas. De manera más reciente, también se contrajeron nuevos compromisos principalmente en los que tiene que ver con la protección de los usuarios de redes sociales, la eliminación de contenido, desactivación de cuentas y la tutela de los derechos del consumidor.

Otro modelo a nivel internacional, es el que se ha generado en Estados Unidos, donde el tratamiento jurídico aplicado a este tipo de plataformas se fundamenta en la autorregulación. Las principales áreas donde se ha volcado la atención de régimen normativo han estado en la protección de datos, comercio electrónico, spam y seguridad.

En cuanto a redes sociales se suscribió el acuerdo titulado "*Joint statement on key principles of social networking sites safety"* o declaración conjunta sobre los principios fundamentales de seguridad en las redes sociales realizado entre Facebook, my space, en busca de proteger a los niños, niñas y adolescentes del contenido subido a las mismas por adultos, así como evitar la comisión de otro tipo de delitos con esta población de especial protección.

Y finalmente el modelo implementado en Latinoamérica se considera un modelo mixto, porque toma algunos elementos del europeo y otros del estadounidense, y se caracteriza principalmente por su flexibilidad, incipiente normatividad, presencia de organismos públicos y privados que coadyuvan a regular internet y la inserción de leyes sobre derechos de autor progresivamente.

Capítulo 3. Responsabilidad de medios por parte de las operadoras de redes sociales y sus efectos jurídicos

3.1 Naturaleza de la responsabilidad de medios

3.1.1 Distinción entre obligaciones de medios y obligaciones de resultados

La clasificación que se realiza de las obligaciones permite distinguir algunas situaciones jurídicas muy precisas, que permiten establecer el surgimiento de la responsabilidad civil. En el caso de las obligaciones de medios y de resultados no es la excepción, pues ambas modalidades contienen una serie de criterios y efectos jurídicos, que requieren un especial análisis para la exposición del problema de investigación.

Bajo esta pequeña introducción, se ha podido encontrar que las obligaciones de medios y de resultados, se encuentran especialmente desarrolladas en el área de la doctrina y la jurisprudencia, por cuanto se fijaran algunas distinciones dadas en estos dos escenarios. Inicialmente es preciso definir según la Corte Suprema de Justicia, las obligaciones de medios como aquella que se da en medio del azar o en la que el acaso es parte constitutiva de su contenido. En las obligaciones de medio el resultado no depende de la actuación diligente del deudor. (Corte Suprema de Justicia. Sala Civil. Sentencia 001 de 30 de enero de 2001, expediente 5507)

Por su parte en las obligaciones de resultado, el interés primario del titular del derecho crediticio sí se puede obtener con el comportamiento o conducta debida, toda vez que en ellas la presencia del componente aleatorio o de azar es exigua, y por ende, el deudor sí puede garantizar

que el acreedor obtenga el resultado o logro concreto que constituye dicho interés primario. (Corte Suprema de Justicia, Sala Civil. Sentencia de 5 de noviembre de 2013, expediente 00025)

De acuerdo con la doctrina citada por Lobato, 1992:

> Se entiende por obligación de media aquella obligación en la cual la prestación debida consiste en el despliegue de una actividad del deudor, dirigida a proporcionar, de forma mediata, la satisfacción del interés del acreedor, o lo que es lo mismo, en el desarrollo de una conducta diligente encaminada a conseguir el resultado previsto por el acreedor al contratar.
>
> Por el contrario, se entiende por obligaciones de resultado aquéllas en las que el deudor se obliga de forma directa e inmediata a la satisfacción del interés del acreedor, mediante la obtención de un resultado pactado que integra la prestación, un resultado que está in obligatione. Por tanto, su cumplimiento o incumplimiento dependerán directamente de la producción o no del resultado y, en cierta medida, serán independientes del grado de diligencia que emplee el deudor en el cumplimiento de la obligación

3.1.2 Las obligaciones de medios de las operadoras de redes sociales

La Constitución Política de 1991, afirmó en el marco del artículo 15 que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. (Const, Art. 15)

En el marco de esta disposición, se establece el derecho del que gozan los ciudadanos para conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (Const, Art. 15)

Y se dispone además, que en lo referente a la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. (Const, Art. 15) Conforme a lo anterior, se garantiza en el espectro constitucional, el derecho al habeas data, encontrando su protección jurídica en el marco de las leyes 1266 de 2008 y 1581 de 2012, así como en las demás normas concordantes.

Sin embargo, en los últimos cuatro las redes sociales se han convertido en una verdadera tendencia y herramienta para la circulación de datos personales que gozan de un alto grado de protección jurídica, pero que se ven amenazados por la insuficiencia de mecanismos jurídicos para su limitación en materia de autodeterminación informática, toda vez que las políticas de seguridad emitidas en estas plataformas, siguen acreditándose la circulación de la información, bajo la credencial de autorización cuando se firma el contrato de registro en la red social, lo que nos lleva a preguntarnos ¿De qué manera resulta utópica la protección de los datos personales captados por las redes sociales en Colombia?

Al analizar y buscar una respuesta a la pregunta formulada, se encontró que en la jurisprudencia de la Corte Constitucional a través de la Sentencia SU-420 de 2019, por primera se comienzan a imponer límites sobre los malos manejos que se le ha dado a los contratos que suscriben los usuarios con los operadores de las redes sociales, especialmente en lo que tiene que ver con la expresiones que atentan con el derecho a la honra y al buen nombre, así como algunos

indicios para que impute responsabilidad a las plataformas de internet encargadas de administrar dichas herramientas a través de las cuales se realizan las respectivas publicaciones o se comparte contenido.

En el estudio de la Corte Constitucional se afirmó que los operadores de las redes sociales deben prever mecanismos que permitan la remoción del contenido objeto de litigio cuando las autoridades competentes así lo requieran. Es decir, que según el Alto Tribunal cuando el directamente responsable se niegue a comparecer al proceso, deberá entonces el administrador de la red social hacerlos para que se ejecute la parte resolutiva de la sentencia, es decir, que se elimine el contenido que ha generado la violación o vulneración de un derecho.

A partir de esta primera afirmación, se puede inferir que para la Corte Constitucional es prevalente la libertad de expresarse a través de las redes sociales, sobre lo que pudiese configurarse como la responsabilidad de resultados que se le debe imponer a los administradores de estas plataformas digitales, al no contar con una regulación jurídica más estricta, no establecer mecanismos de alerta y ser los encargados del tratamiento de datos personales, que como se ha visto en el contexto internacional implica una serie de responsabilidad bien complejas para dichas operadoras.

Sin embargo, lo cierto es que las redes sociales siguen siendo una bola de fuero en el escenario juridico, que se pasa no llega aun al Congreso de la República y que mientras tanto sigue siendo invicta en el escenario de la jurisprudencia.

No obstante, en un reciente estudio de la Corte Suprema de Justicia mediante Sentencia SC-52382019 del 10 de diciembre del 2019 de la Sala de Casación Civil afirmó que inicialmente no es posible que exista responsabilidad por los comentarios que son dejados en un blog. Sin embargo, cuando el comentario resulta ser ofensivo, inmoderado, injurioso o calumnioso, o también cercena la esfera de la honra y el honor de la personal, entonces los responsables de la administración de estos escenarios digitales, deberán restringir o evitar publicar tales opiniones cuando sean manifiestamente ofensivos, o en su defecto, a eliminarlos en caso de no tener conocimiento efectivo de los mismos; y si ya fueron difundidos, actuar con suma diligencia para retirarlos prontamente o imposibilitar su acceso. No hacerlo, edificaría una responsabilidad civil por culpa probada…". (Corte Suprema de Justicia, SC-52382019 del 10 de diciembre del 2019)

Frente a la posición de la Corte Suprema de Justicia, se puede establecer una teoría diversa al planteamiento expuesto por la Corte Constitucional, pues según este primer Alto Tribunal, cuando se constituyan escenarios como los expuestos en dicha providencia, es posible la imputación de responsabilidad civil. En línea con lo anterior es posible en Colombia la imputación de responsabilidad civil a las empresas operadoras de las redes sociales, bajo los criterios descritos por la Corte Suprema de Justicia, y de donde la Corte Constitucional afirma que no es posible tal responsabilidad.

Sin embargo, a partir de los criterios legales sobre los cuales se sustenta la responsabilidad civil en Colombia, es cierto que es posible imputar responsabilidad civil a los operadores de redes sociales, pero una responsabilidad civil de medios, que como se analizó en el primer apartado de este capítulo, su cumplimiento e incumplimiento son independientes de la

obtención del resultado esperado por el acreedor y dependen únicamente de la actuación diligente o negligente del deudor.

Dicho criterio se encuentra fundado en que para el legislador y tribunales colombianos, el contrato que se suscribe para el uso y acceso a las redes sociales es de tipo gratuito, y por lo tanto se puede imputar solo responsabilidad de medios, sin embargo, dichos razonamientos resultan diversos pues en la realidad, cuando el usuario suscribe un contrato con una red social y acepta las condiciones de uso y privacidad, le está entregando un bien ampliamente protegido por el régimen juridico interno y externo, como es la información personales o datos personales, para que haga uso y tratamiento de los mismos, convirtiéndose entonces en un contrato oneroso, del cual no se puede derivar una responsabilidad civil de medios, sino de resultados, endilgada además hasta por culpa leve.

Capítulo 4. La culpa grave en las empresas operadores de redes sociales y sus efectos jurídicos en Colombia

4.1 Estadios de la Culpa

De conformidad con la doctrina jurídica, la culpa es "un error de conducta tal, que no lo habría cometido una persona cuidadosa situada en las mismas circunstancias externas que el autor del daño". En Colombia, la legislación civil reconoce tres estadios de la culpa. La primera de ellas, es la culpa grave, la culpa leve y la culpa levísima. Al respecto, el artículo 63 nos indica que:

La culpa grave o también denominada negligencia grave, es aquella que ocurre cuando no se manejan los negocios ajenos con el debido cuidado, de forma negligente o poco prudente. En materia civil, la culpa grave equivale al dolo.

El siguiente estadio es conocido como la culpa leve, y hace referencia a un descuido ligero o falta de cuidado que emplean los hombres en sus negocios propios. . Esta especie de culpa se opone a la diligencia o cuidado ordinario o mediano.

Y finalmente encontramos la culpa levísima, considerada como la falta de aquella esmerada diligencia que un hombre juicioso emplea en la administración de sus negocios importantes. Esta especie de culpa se opone a la suma diligencia o cuidado. (Código Civil, Art. 63)

4.2 La culpa grave en las operadoras de redes sociales

La culpa configura uno de los elementos que constituyen la responsabilidad civil y como consecuencia la obligación de reparar el daño. Sin embargo, no son solo estos los elementos que concurren, puesto que no solo basta con haber causado el daño, sino que además se requiere que dicha conducta haya sido efectuada con culpa, que a su vez goza de una clasificación o estadios que van desde la culpá grave hasta la levísima, y que según algunos criterios jurídicos, se imputa solo por la conducta ocurrida con culpa grave.

Dentro del régimen civil colombiano, la imputación de responsabilidad civil de medios, se da hasta por culpa grave, exonerándose la culpa leve y levísima de este escenario. Así las cosas, al platear este escenario sobre el análisis o la pregunta de investigación es posible concluir que efectivamente en Colombia resulta utópica la protección de los datos personales a través de las redes sociales, toda vez que el mismo sistema juridico es incapaz de proveer a los ciudadanos de mecanismos jurídicos para su protección, tal como lo evidencian los vacíos jurídicos en materia de protección a los usuarios.

Pero no solo es eso, al imputarse en el escenario de la responsabilidad que le asiste a los operadores de las redes sociales, la culpa grave, sin que se tengan en cuenta siquiera la culpa leve, se permite que dichos operadores puedan hacer uso de los datos personales, exonerándose de su deber de reparar, solo por el hecho de contar con condiciones mínimas en sus contratos de uso y privacidad, y dejando a los usuarios en una situación claramente desventajosa frente a la imponente fuerza y poder de los grandes como Facebook, Twitter y demás plataformas digitales.

Al analizar la culpa grave en materia de responsabilidad civil de los operadores judiciales, se prevé un escenario en el cual se exige que el usuario pruebe el daño, y que se obligue a su reparación, no obstante la exclusión de las otras dos tipologías, permite que estas plataformas continúen captando datos personales con la venia jurídica de los Estados, que a su vez están obligados a velar por la protección de la información personales de los ciudadanos, lo que a su vez pudiese verse en otro análisis más profundo como una responsabilidad del Estado frente a la regulación de redes sociales.

Conclusiones

El mundo de las redes sociales durante la última década ha crecido a un ritmo vertiginoso, encontrándose que el manejo y el intercambio de datos personales se efectué a través de estas mismas y que por ende el derecho tenga que avocarse a la regulación de su uso, teniendo en cuenta que se hace tránsito de información personal o datos personales, que encuentran un amplio blindaje juridico a nivel internacional.

En el caso de Colombia, a partir de la promulgación de la Carta Política de 1991, se establece un régimen de protección en materia de datos personales, a través del artículo 15, y las posteriores normas que han venido indexando mecanismos de protección desde el ámbito penal, civil y demás. Sin embargo, el manejo de las redes sociales y su autorregulación por parte de sus operadores, ha llevado al descuido por parte del legislador para implementar normas que regulen el delicado tratamiento que se le asigna a los datos personales a través de las redes sociales, máxime cuando el usuario no cuenta con mecanismos legales que aporten mayor protección a sus derechos.

Tras analizar esta situación jurídica, se podido determinar que en Colombia si resulta utópica la protección de los datos personales a través de las redes sociales, por cuanto el mismo sistema normativo y jurisprudencial desconoce la necesidad de regular el uso y manejo de las redes sociales; adicionalmente, en materia de responsabilidad de los operadores la jurisprudencia aún se encuentra en discrepancias sobre la imputación o no de esta, y quienes ya lo han concebido, como es el caso de la Corte Suprema de Justicia, entonces lo hacen desde el tipo de responsabilidad de medios, donde lamentablemente se concibe el contrato entre usuarios y

operadores de redes sociales como un contrato gratuito, en el que debe obrar la culpa grave para su debida imputación.

Finalmente, es preciso concluir que cuando se habla del contrato que se suscribe con las redes sociales, no se trata de un contrato solemne sino de un contrato consensual, que adicionalmente requiere que se modifique la percepción del tipo de contrato suscrito con las operadoras de redes sociales y los usuarios, el cual no corresponde a un contrato gratuito sino de tipo oneroso, en este sentido solo podrá imputarse responsabilidad por culpa grave.

Referencias

Celaya, J. (2008). *La Empresa en la WEB 2.0.* España: Editorial Grupo Planeta España .

Código Civil, Art. 63, Diario Oficial No. 2.867 de 31 de mayo de 1873. Recuperado el 2022, de http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr001.html#63

Congreso de Colombia, Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información . Recuperado el 2022, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de Colombia, Ley 1336 de 2009, Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. (Diario Oficial No. 47.417 de 21 de julio de 2009). Recuperado el 2022, de https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

Congreso de Colombia, Ley 1620 de 2013, por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. Recuperado el 2022, de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685356

Congreso de Colombia, Ley 599 del 2000, Por la cual se expide el Código Penal (Diario Oficial No. 44.097 de 24 de julio de 2000). Recuperado el 2022, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de Colombia, Ley 733 del 2002, por medio de la cual se dictan medidas tendientes a erradicar los delitos de secuestro, terrorismo y extorsión, y se expiden otras disposiciones..

Recuperado el 2022, de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1667320

Congreso de la Republica de Colombia, Proyecto de Ley para regular las políticas de uso y apropiación de las redes sociales y se dictan otras disposiciones generales. Recuperado el 2022, de https://www.lafm.com.co/tecnologia/en-que-consiste-el-proyecto-para-regular-las-publicaciones-en-redes-sociales

Consejo de Europa, Convenio 108 de 1981, El Convenio n.o 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ám. Recuperado el 2022, de https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales#:~:text=El%20Convenio%20n.&text=108%20del%20Consejo%20de%20Europa,de%20la%20protecci%C3%B3n%20de%20datos.

Consejo de Europa. (1981).Convenio 108. para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Recuperado el 2021, de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf

Const, Art. 15.

Constitucion Politica de 1991. (s.f.). Recuperado el 2021, de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Constitución Política de Colombia, 1991, Art. 61. Recuperado el 2022, de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Corte Constitucional, 1995,Sentencia SU-082 (MAGISTRADO PONENTE: JORGE ARANGO MEJIA.). Recuperado el 2022, de https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Corte Constitucional, 2002, Sentencia T-729, Referencia: expediente T-467467 (Magistrado Ponente: Dr. EDUARDO MONTEALEGRE LYNETT). Recuperado el 2022, de https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Constitucional, 2002, Sentencia T-729 (Magistrado Ponente: Dr. EDUARDO MONTEALEGRE LYNETT). Recuperado el 2022, de https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Constitucional, 2012, Sentencia T-414 (Magistrado Ponente: MAURICIO GONZÁLEZ CUERVO). Recuperado el 2022, de https://www.corteconstitucional.gov.co/RELATORIA/2012/C-414-12.htm#:~:text=C%2D414%2D12%20Corte%20Constitucional%20de%20Colombia&text=La%20jurisprudencia%20de%20la%20Corte,fuentes%20ex%C3%B3genas%20y%20fuentes%20end%C3%B3genas.

Corte Constitucional, 2019, Sentencia SU-420, Referencia: Expedientes T-5.771.452, T-6.630.724, T-6.633.352 y T-6.683.135. (Magistrado Ponente: JOSÉ FERNANDO REYES CUARTAS). Recuperado el 2022, de https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm

Corte Constitucional, Sentencia C-1011 de 2008, Referencia: expediente PE-029 (Magistrado Ponente: Dr. JAIME CÓRDOBA TRIVIÑO). Recuperado el 2022, de https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional, Sentencia de Unificación 082 de 1995, REF: PROCESO T- 40.966 (MAGISTRADO PONENTE: JORGE ARANGO MEJIA.). Recuperado el 2021, de https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Corte Suprema de Justicia, Sala Civil. Sentencia de 5 de noviembre de 2013, expediente 00025.

Corte Suprema de Justicia, SC-52382019 del 10 de diciembre del 2019, Radicación: 76001-31-03-015-2011-00088-02 (M.P. LUIS ARMANDO TOLOS A VILLABONA). Recuperado el 2022, de https://cortesuprema.gov.co/corte/wp-content/uploads/2019/12/SC5238-2019-2.pdf

Corte Suprema de Justicia. Sala Civil. Sentencia 001 de 30 de enero de 2001, expediente 5507.

Cuervo, A. J. (2014). *Autodeterminacion Informativa.* Recuperado el 2021, de http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/

Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana (Red Iberoamericana de Proteccion de Datos 2006). Recuperado el 2022, de http://www.transparencia.udg.mx/sites/default/files/Directrices%20para%20la%20armonizaci%C3%B3n%20de%20la%20protecci%C3%B3n%20de%20datos%20en%20la%20Comunidad%20Iberoamericana.pdf

Gonzalez, L. (2010). *Responsabilidad Legal en Redes Sociales en Internet.* .

Jacome, N. L., & Villamil, M. M. (2020). *La Utopía de la Intimidad en los Contratos de las Redes Sociales.* Facultad de Derecho, Universidad Cooperativa de Colombia Campus Cartago. Recuperado el 2021, de https://repository.ucc.edu.co/bitstream/20.500.12494/20600/1/2020_utopia_intimidad_contratos.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 dicta (Congreso de Colombia). Recuperado el 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. (Congreso de Colombia). Recuperado el 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Lobato, G. J. (1992). *"Contribución al estudio de la distinción entre obligaciones de medios y obligaciones de resultado".* Anuario de Derecho Civil.

Organización de Naciones Unidas, Resolucion 45/95, PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE LOS FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES. Recuperado el 2022, de http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Superintedencia de Industria y Comercio. (2018). *Como medida preventiva, Superindustria ORDENA bloqueo de aplicación Pig.gi por su aparente vinculación con posible tratamiento ilegal de datos personales de colombianos.* Recuperado el 2021, de https://www.sic.gov.co/noticias/como-medida-preventiva-superindustria-ordena-bloqueo-de-aplicacion-pig-gi-por-su-aparente-vinculacion-con-posible-tratamiento-ilegal-de-datos-personales-de-colombianos