PROYECTO DE TRABAJO DE GRADO

PROTECCIÓN DE DATOS PERSONALES EN LOS SERVICIOS DE INTERNET

CARMEN CAROLINA SOTO ESPINOSA

CAMILO ANDRES DUCUARA CUERVO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C, DICIEMBRE DE 2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

En la actualidad con las nuevas tendencias derivadas de la práctica internacional de la información, resulta relevante atender las necesidades de la visión global de la misma, lo cual ha implicado la creación de nuevos escenarios legales, con el fin de dar solución ágil a las relaciones informáticas; por lo cual los diferentes actores de naturaleza privada y pública han orientado importantes esfuerzos para lograr los fines propuestos al interior de sus diferentes corporaciones, adquiriendo en gran medida diversidad de beneficios en materia de información.

Por lo tanto, el mundo hiperconectado actual favorece en gran medida la totalidad de las actividades diarias de la población mundial, sin embargo, este favorecimiento constituye en sí mismo la piedra angular del debido uso de información, debido a que en la habitualidad del uso de la información resultado del principio de inmediatez, la población desconoce los contenidos y alcances producto del servicio de internet diariamente utilizados.

La habitualidad de la información implica el suministro de diversidad de datos, compuestos en información e identificación, e incluso información sensible. Una vez son registrados estos datos el titular de la información pierde el control del tratamiento que ejecuta el depositario de estos, es decir, al trasladar contenido se desdibuja fácilmente el imperio de los datos, lo cual repercute en la protección legal y su aplicabilidad en el ciber espacio.

En este sentido, resulta manifiestamente necesario analizar la procedencia y efectividad del marco regulatorio del tratamiento de datos a la luz de legislación colombiana, con lo cual el presente proyecto de investigación se dividirá en tres grandes etapas; la primera de ellas comprenderá la naturaleza de los servicios que provee internet y su relación con los datos que se alojan en el ciber espacio, por otro lado, se formula una investigación de carácter reflexivo de la exposición y el riesgo del tratamiento de datos que se alojan en el ciber espacio a la luz del tratamiento internacional, especialmente el caso Europeo. Como tercera etapa se expondrá sustancialmente el estado actual del marco regulatorio de la protección de datos en Colombia, y su eficacia al estado actual de la práctica informática doméstica, en cumplimiento de los fines constitucionales, legales y reglamentarios del estado social de derecho.

A nivel internacional, por ejemplo, en mayo de 2018 entró en vigencia el reglamento general de protección de datos en la unión europea; el cual fue aprobado desde mayo de 2016 y cuyo objetivo es proteger a las personas en lo que respecta a sus datos personales y la circulación de éstos. Este es un claro ejemplo de cómo a nivel mundial se ha avanzado en la rigurosidad de la legislación para la salvaguarda de la información de los ciudadanos.

1 GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

El presente proyecto se desarrolla bajo la línea de investigación *Software inteligente y convergencia tecnológica,* pues se abarcan temas relacionados con el auge de algunos de los servicios de internet más utilizados.

1.2 PLANTEAMIENTO DEL PROBLEMA

Diariamente los ciudadanos exponen su información en internet para hacer uso de herramientas del día a día como lo son redes sociales y correo electrónico, entre otras. Esto representa un riesgo para su información porque pese a aceptar las condiciones de uso de estos servicios, la realidad es que la mayoría de los usuarios ignoran qué es lo que en realidad están aceptando, y el uso que los dueños de estas herramientas le están dando a los datos recolectados. Normalmente los servidores de estos servicios se encuentran en diferentes países, por lo que es complejo determinar qué leyes aplican para la protección de la información; por lo anterior es importante dar una mirada reflexiva al buen uso de los datos personales que Colombia ha regulado y su cumplimiento cuando se abordan nuevos escenarios como el ciberespacio.

En concordancia con la ley de protección de datos personales y los temas concernientes a seguridad de la información de cada uno de los ciudadanos colombianos, es necesario analizar cuáles son las políticas de tratamiento de datos o “términos y condiciones de uso” que los proveedores de servicios en internet están poniendo a disposición de sus usuarios y su alineación con las disposiciones que Colombia ha regulado al respecto. Razón por la cual este proyecto persigue la realización de una comparación entre el cumplimiento o desviación de los mismos respecto a la regulación que Colombia ha impartido en la materia.

1.2.1 **Antecedentes del problema**

Actualmente en Colombia, se ha reglamentado el derecho a la intimidad respecto al tratamiento de los datos personales en dos grandes leyes:

La expedición en el año 2008 de la ley 1266 "Habeas Data", *"… 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".*(Congreso de la república, 2008)

Y por otra parte la ley 1581 de 2012, se reguló la protección de datos personales en lo concerniente a la información de los ciudadanos en bases de datos y archivos. El objeto de la ley "es *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.* ".(Congreso de la república, 2012)

Sin embargo, en las leyes mencionadas anteriormente, no se hace referencia a los lineamientos del manejo de la información en el ciberespacio, por cuanto específicamente el ámbito de aplicación de la ley 1581 de 2012 se define en el artículo 2 : "*La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales*" (Congreso de la república, 2012)

A nivel mundial se han generado estudios concernientes al tema tratado en este proyecto de investigación: (Pazos Castro, 2015) estudió los procesos que realizan los motores de búsqueda en internet y los datos personales disponibles en la red. En este artículo, el autor después de definir el concepto de datos personales basándose en las directrices del parlamento europeo, hace un análisis sobre la posibilidad que tienen los motores de búsqueda para explotar económicamente los datos personales de los usuarios basándose en sus búsquedas. También, el autor analiza la facilidad que tienen los internautas para encontrar información personal de terceros cuando hacen uso de estos motores de

búsqueda.

Por otro lado, (Moreno Muñoz, 2014) en su estudio resalta el riesgo que tienen los derechos a la intimidad y privacidad en internet con amenazas como las agencias de seguridad nacional e inteligencia de los gobiernos.

A nivel internacional, uno de los casos más reconocidos de violación a la privacidad de las personas en internet, fue el que sucedió en abril de 2018 en la red social Facebook en el que se vio involucrado su fundador, Mark Zuckerberg, al revelarse que en la campaña presidencial de 2016 en Estados Unidos hubo acceso no autorizado por parte de la firma de consultoría Cambridge Analytica a la cuenta de unos 87 millones de usuarios para influir en su decisión de voto. Éste es un claro ejemplo de cómo los usuarios exponen su información a terceros aún después de haber aceptado los términos y condiciones de ésta red social; o incluso de cómo la información personal puede verse comprometida por la inoperancia de éstos términos y condiciones.

1.2.2 **Pregunta de investigación**

Pregunta general:

¿Es eficaz la normatividad vigente del estado colombiano sobre la protección datos personales en el ciber espacio?

Preguntas específicas:

- ¿Cuál es la naturaleza de los datos personales que son tratados por los servicios de internet?
- ¿El marco jurídico de la protección de datos en Colombia, con relación al respeto de los derechos fundamentales, responde a las necesidades actuales de los medios masivos de internet?
- ¿Cuál es el nivel de protección existente con relación al derecho a la intimidad de la población colombiana en los servicios de internet?
- ¿Cuál es el nivel de intervención estatal que se requiere para garantizar la salvaguarda de los derechos suministrados por los titulares en internet?

1.2.3 **Variables del problema**

1.3 JUSTIFICACIÓN

En la actualidad, con las crecientes necesidades del mundo globalizado y las nuevas tendencia de la híper-conexión, el estado colombiano se vio obligado a expedir la ley 1266 de 2008 sobre habeas data, la ley 1581 de 2012 sobre protección de datos personales, con las cuales se pretende regular la totalidad de las actividades de tratamiento de datos de la población colombiana.

Sin embargo, la realidad actual después de seis años de expedición legal, radica en no evidenciar la estandarización del estado colombiano a las necesidades internacionales, he incluso catalogar a Colombia como un país que no cuenta con un nivel adecuado de protección de datos, ejemplo de ello se encuentra la negativa a Colombia de la declaración de nivel de protección adecuado de la Comisión Europea, la cual en la actualidad representar ser el marco legal pionero en protección de datos, al garantizar el mayor nivel de garantía a sus asociados.

Por lo cual resulta manifiestamente necesario materializar la presente investigación de naturaleza exploratoria, encaminada a resaltar el estado actual de exposición de la información de datos de diferente naturaleza de las personas, los cuales deben responder al criterio de confidencialidad de la información intrínsecamente ligado al derecho a la intimidad, cuando se accede a los servicios expuestos de internet.

1.4 OBJETIVOS

1.4.1 **Objetivo general**

Analizar la situación actual del cumplimiento del derecho a la intimidad en internet, mediante un estudio que permita evidenciar debilidades y fortalezas de la legislación colombiana en la protección

de datos frente a las políticas, términos y condiciones de los servicios ofrecidos en la web.

1.4.2 Objetivos específicos

1.4.2.1 Identificar los tipos de datos personales que se almacenan en los servicios que se prestan en internet, una vez son aceptados los términos y condiciones.

1.4.2.2 Realizar un estudio comparativo para conocer el nivel de cumplimiento de los servicios de internet respecto a la regulación colombiana en materia de protección de datos personales.

1.4.2.3 Determinar cuáles son las debilidades y fortalezas de la legislación colombiana, orientadas a la salvaguarda del derecho fundamental a la intimidad en el ciberespacio.

1.4.2.4 Proponer mecanismos que permitan a los ciudadanos proteger la confidencialidad, integridad y disponibilidad de la información que suministran en aplicaciones en internet.

2 MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

2.1.1 **Ciberespacio:** Es una construcción metafísica compuesta por hardware digital, los datos que éste hardware crea y administra, y los humanos que producen y consumen la información contenida en los datos y que interactúan con el hardware. Se reconoce a los humanos como responsables de la dinámica del sistema, así como lo son los datos y la tecnología. (Edgar & Manz, 2017)

2.1.2 **Ciberidentidad:** Hace referencia al conjunto de características de las personas que las diferencian de otras, en el ciberespacio (Edgar & Manz, 2017).

2.1.3 **Ciberseguridad:** Edgar & Manz (2017) definieron este concepto como el conjunto de medidas y acciones tomadas para evitar el acceso no autorizado, la manipulación o destrucción de datos cibernéticos; incluyendo tecnologías, políticas y procedimientos para asegurar algo en el ciberespacio.

2.1.4 **Dato personal**: Toda información relacionada que identifica o hace identificable a una persona (Parlamento Europeo & Consejo de la Unión Europea, 2018).

2.1.5 **Datos íntimos o privados:** Son datos que se caracterizan porque le pertenecen al titular y son únicamente de su interés; sólo pueden ser obtenidos con su consentimiento, por orden de autoridad judicial y para salvaguardar la vida de la persona cuando ésta se encuentre en incapacidad física o jurídica. Los ejemplos más comunes son creencias religiosas, orientación sexual o afecciones a la salud. (Superintendencia de industria y comercio, 2014)

2.1.6 **Datos públicos:** En Colombia, la Superintendencia de Industria y Comercio (SIC) define los datos públicos como todos aquellos datos que tienen un interés general, como por ejemplo el número de cédula, sentencias judiciales, etc.

2.1.7 **Datos semiprivados:** Son datos que aun teniendo carácter privado, son de interés únicamente del titular y a un grupo determinado de personas, las cuales pueden consultar la información con autorización del titular. El ejemplo más frecuente es el historial crediticio de una persona. (Superintendencia de industria y comercio, 2014)

2.1.8 **Encargado del tratamiento:** La Superintendencia de Industria y Comercio en Colombia, SIC, define el en cargado del tratamiento de datos personales como *"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos"*("Políticas de tratamiento de la información personal en la superintendencia de industria y comercio," 2014)

2.1.9 **Geolocalización:** Es un conjunto de tecnologías que tienen como fin la utilización de la información relacionada con la ubicación geográfica del mundo real ("Características de la geolocalización Online," 2017).

2.1.10 **Gestión de riesgos de seguridad digital:** En el CONPES 3854, se define como el conjunto de actividades coordinadas en una organización para abordar el riesgo de seguridad digital

(CONPES, 2016).

2.1.11 **Habeas data**: Según la SIC, es el derecho que tienen los ciudadanos de acceder a sus datos, corregirlos y actualizarlos.

2.1.12 **Ciudadanos residentes y domiciliados:** Basándose en la definición para efectos tributarios, un extranjero se considerará residente cuando permanezca en territorio colombiano durante 183 días, continuos o no, dentro de un período de 365 días. Los ciudadanos domiciliados son aquellos que residen permanentemente en Colombia ("Instituto Nacional de Contadores Públicos" 2015).

2.1.13 **Nube:** Es un modelo que traslada la información de los usuarios a un conjunto de servidores a los que se accede a través de una red, frecuentemente internet. (Mell & Grance, 2011).

2.1.14 **Responsable del tratamiento:** *"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos"*("Políticas de tratamiento de la información personal en la superintendencia de industria y comercio," 2014)

2.1.15 **Riesgo de Seguridad digital:** Describe una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital, resultante de la combinación de vulnerabilidades y amenazas en el ambiente digital. El riesgo de Seguridad digital puede debilitar el logro de objetivos económicos y sociales (CONPES, 2016).

2.1.16 **Términos y condiciones:** Son un conjunto de políticas que rigen el uso que se le da a un sitio web, así como el acceso a los contenidos que se encuentran allí disponibles (Edgar & Manz (2017).

2.1.17 **Transmisión y transferencia de información:** Basándose en el principio de Responsabilidad demostrada, la transmisión hace referencia a que el responsable de la

información determina el tratamiento de los datos personales por parte del encargado; mientras que en la transferencia el encargado decide el tratamiento que le dará a los datos personales que le ha entregado el emisor ("Diferencias entre transmisión y transferencia de datos personales," 2017).

2.2 MARCO TEÓRICO

Dado que el presente trabajo de investigación se enfoca en la exposición de los datos de los usuarios en los servicios prestados en internet, es fundamental identificar cuáles son los tipos de datos que existen; así como tener claro a qué se hace referencia cuando se menciona un servicio de internet. También se debe realizar una contextualización sobre cómo se encuentra la legislación colombiana relacionada con la protección de datos personales con respecto a la legislación internacional; facilitando la verificación del cumplimiento de éstas leyes frente a los términos y condiciones de los servicios prestados en la web.

Cuando se habla de estos servicios, se hace referencia a aquellas herramientas de uso diario utilizadas con diferentes fines; como lo son las redes sociales, el correo electrónico y las plataformas para almacenamiento en la nube.

En la figura 1 se relacionan los tipos de datos personales que existen y su exposición en los servicios prestados en internet; y la importancia de equiparar la legislación concerniente a los datos personales con los términos y condiciones definidos por los servicios de la web descritos en el alcance de este proyecto.

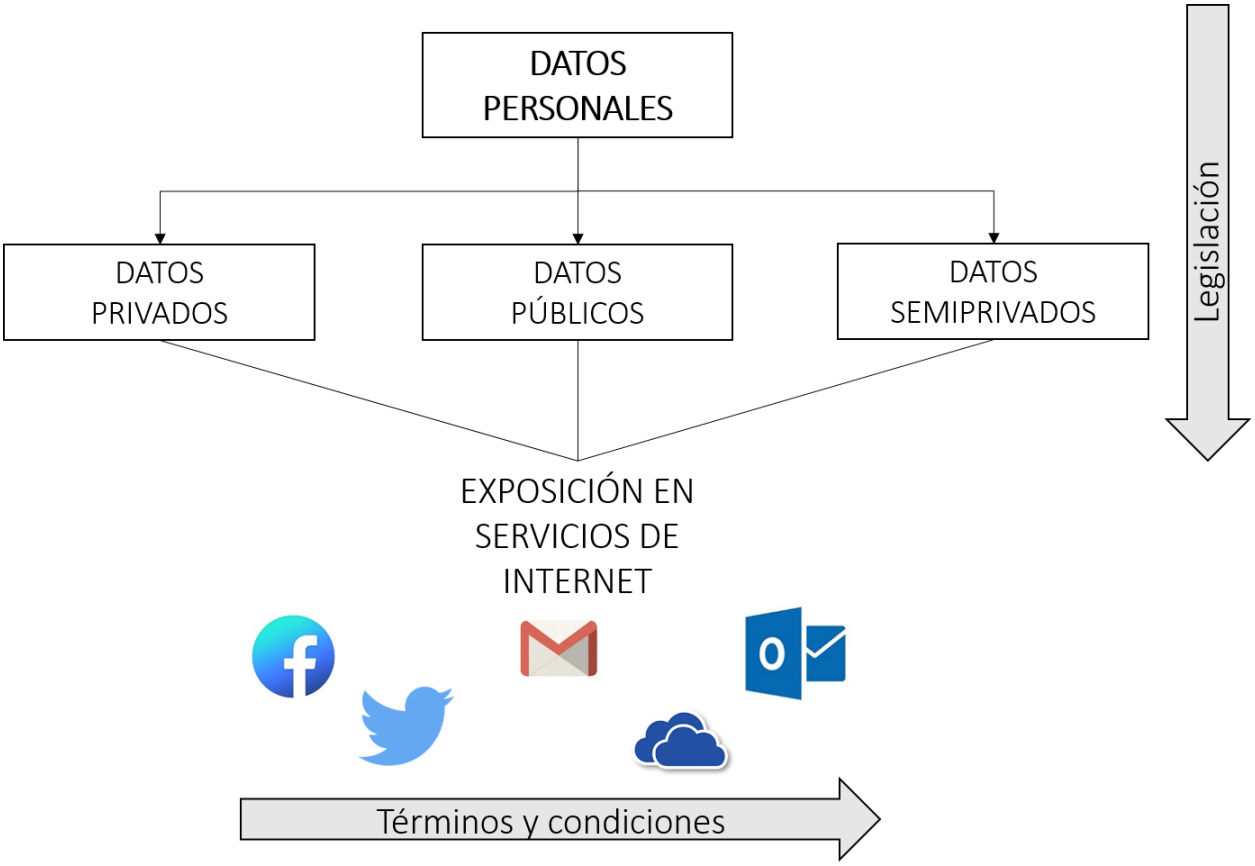

Figura 1: Legislación Vs. Términos y condiciones. Fuente: Elaboración propia.

Actualmente, los datos personales y la información en general son considerados como activos económicos clave, lo cual representa un desafío para las autoridades legislativas que deben velar por el cumplimiento del derecho a la intimidad y al mismo tiempo garantizar que el uso que las diferentes entidades u organizaciones le den a la información de los ciudadanos sea el apropiado, y se haga con el consentimiento de los dueños de la información. Sin embargo, el concepto de propiedad de los datos personales tiene algunas reservas a nivel internacional, pues tiene implicaciones importantes para el futuro de la economía digital y el comercio de datos; razón por la cual recientemente ha surgido el concepto de propiedad de datos como un derecho legal a nivel de la Unión europea (Janeček, 2018).

Janeček afirma que puede presentarse una discusión y es los datos son un objetivo móvil; lo que significa que los que ahora se consideran personales pueden convertirse en no personales gracias a los grandes avances tecnológicos y analíticos en los que la sociedad está inmersa día a día. Esta situación da lugar a un debate interesante sobre a cuáles datos específicos se les debería aplicar la legislación vigente; y sobre cómo el dinamismo de la clasificación de los datos podría modificar las leyes actuales o

dar lugar a la expedición de algunas nuevas.

Hoy en día es muy común encontrarse con que los motores de búsqueda almacenan las consultas realizadas por los usuarios, lo que permite rastrear el equipo desde donde se están realizando estas consultas recordando el interés de cada persona. Los motores de búsqueda generalmente son gratuitos y el aprovechamiento de estos servicios implica la renuncia al derecho a la intimidad o la disminución del alcance del mismo. Similarmente ocurre con otros servicios de internet como las redes sociales, el correo electrónico y los servicios de almacenamiento en la nube. Estas actividades permiten vender la información de los intereses de los usuarios a campañas publicitarias, medios de comunicación, etc. Sin embargo, el problema se presenta cuando esta misma información es utilizada con fines indeseables para las personas, como por ejemplo el robo de sus cuentas bancarias a través de phishing, entre otros (Şerbu & Rotariu, 2015).

En la actualidad, la informática es considerada la quinta utilidad más importante después del agua, la electricidad, el gas y la telefonía (Cheng & Lai, 2012); lo cual, y gracias a los importantes avances tecnológicos del día a día, ha despertado interés en desarrollar servicios de computación en la nube. Actualmente están definidos cuatro modelos de implementación de nube (Mell & Grance, 2011): nube privada, nube comunitaria, nube pública y nube híbrida. La nube privada está destinada únicamente para una organización, mientras que la pública es para el público en general. La nube comunitaria se conforma por un conjunto de organizaciones con intereses en común; y la híbrida es una composición de los modelos de nube ya descritos (Cheng & Lai, 2012). El crecimiento de servicios de alojamiento en la nube se suma a los desafíos anteriormente descritos en cuanto a la protección de datos y de la información, pues al ser la nube un medio almacenado en internet, se transfieren todos los riesgos de seguridad de internet a este medio. Además se presentan otras implicaciones, como por ejemplo que la información se almacene y procese en diferentes lugares geográficos alrededor del mundo con diferentes normativas, lo que podría implicar problemas de jurisdicción y cumplimiento legal; que se comparta la infraestructura física entre usuarios; y que los proveedores de servicios de computación en la nube tengan acceso a información de los usuarios, entre otros (Cheng & Lai, 2012).

En este sentido, la Organización para la Cooperación Económica y Desarrollo (OCDE) definió el término de responsabilidad demostrada, *Accountability*, (The Centre for Information Policy Leadership, 2009) para proporcionar una solución a la protección de datos que incluye cinco elementos fundamentales:

- Compromiso de las organizaciones con la responsabilidad y adopción de políticas

internas de acuerdo al contexto externo.

- Mecanismos para poner en práctica políticas de privacidad, incluyendo herramientas de capacitación y educación.
- Sistemas para revisiones internas, con supervisión continua y aseguramiento de verificación externa.
- Transparencia y mecanismos de participación individual.
- Medios para remediación y cumplimiento externo.

El principio de responsabilidad demostrada es muy relevante, ya que su implementación incluye beneficios no solo para los titulares de los datos personales sino también para las organizaciones; permitiéndoles maximizar el uso inteligente de la información, aumentar su nivel de competitividad y consolidar su reputación empresarial (Remolina Angarita & Zuluaga Alvarez, 2018).

El Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) de la facultad de Derecho de la Universidad de Los Andes, publicó una guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos (Remolina Angarita & Zuluaga Alvarez, 2018), cuyo objetivo es el de presentar algunas recomendaciones para el envío de datos personales a otros países, respetando los derechos de los titulares de la información. Esta guía está orientada para que su implementación se realice tanto en Colombia como en los demás países de Latinoamérica. Allí se describen detalladamente las siguientes recomendaciones para implementar el principio de *Accountability* en la transferencia de datos personales.

- *Verificar que se está facultado para transferir datos personales a otros países.*
- *Determinar el mecanismo adecuado que utilizará para transferir o transmitir internacionalmente datos personales.*
- *Establecer como se probaran las medidas de Accountability para transferir datos personales.*
- *Tener en cuenta los objetivos que se deben cumplir según la regulación del su país para transferir datos internacionalmente.*
- *Asegurar el cumplimiento de las finalidades que se deben alcanzar con el principio de Accountability.*
- *Crear estrategias para proteger los intereses de la organización.*
- *Adoptar medidas para no defraudar la confianza de sus clientes o de los titulares de los datos.*

- *Prever las transferencias ulteriores de datos personales.*
- *Incrustar la privacidad desde el diseño y por defecto en las transferencias internacionales de datos personales.*
- *Replicar medidas proactivas del tratamiento de datos personales a las transferencias internacionales de dicha información.*
- *Articular las herramientas de Accountability en un contrato ajustado a las particularidades de cada transferencia.*
- *Articular las anteriores recomendaciones con la guía de Accountability de la autoridad de protección de datos.*

En Colombia, la ley 1581 de 2012 de protección de datos personales en su artículo 26 (Congreso de la república, 2012), regula la transferencia internacional de información. Como regla general, se prohíbe la transferencia internacional de datos a cualquier país que no proporcione niveles adecuados de protección de datos. Estos niveles son adecuados cuando se cumplen los siguientes estándares definidos por la Superintendencia de Industria y Comercio (SIC). ("Transferencia internacional de datos," n.d.)

- *Existencia de normas aplicables al tratamiento de datos personales.*
- *Consagración normativa de principios aplicables al Tratamiento de datos, en otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.*
- *Consagración normativa de derechos de los Titulares.*
- *Consagración normativa de deberes de los Responsables y Encargados.*
- *Existencia de medios y vías judiciales y/o administrativas para garantizar la tutela de los derechos de los Titulares y exigir el cumplimiento de la ley.*
- *Existencia de autoridad (es) pública (s) encargada (s) de la supervisión del Tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares*

La SIC también enlista los países que cumplen con los requisitos para la transferencia de datos personales, de acuerdo con el cumplimiento de los requisitos mencionados anteriormente.

Alemania, Australia, Austria, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia y los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea ("Circular

externa No. 002 de 2018," n.d.).

Además de la transferencia de información, también existe la transmisión de la misma y es muy importante tener en cuenta la diferencia entre estos dos conceptos, entendiéndose la transferencia como la acción de entregar a un tercero la información de manera que el receptor la tratará con independencia del responsable o encargado. Mientras que en la transmisión el receptor tratará la información de acuerdo a las reglas impuestas por el emisor.

Por otro lado, la Organización para la Cooperación y Desarrollo Económico, OCDE, publicó en septiembre de 2015 las Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social. En ese sentido, el Consejo Nacional de Política Económica y Social, en el documento CONPES 3854, define la Política Nacional de Seguridad Digital. Allí se menciona la recomendación de la OCDE sobre distinguir el objetivo de prosperidad económica y social de los objetivos de defensa y seguridad nacional en el entorno digital. Esto significa que los riesgos de seguridad digital no deben verse únicamente como un problema técnico, sino que deben abordarse como un riesgo económico que debe gestionarse como cualquier proceso de toma de decisiones. El CONPES 3854 describe la implementación de esta política a través de los siguientes objetivos (CONPES, 2016):

- *Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.*
- *Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital*
- *Fortalecer la seguridad de los individuos y del Estado en el entorno digital, y nivel nacional y transnacional, con un enfoque de gestión de riesgos.*
- *Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.*
- *Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.*

2.3. Marco jurídico

En Colombia existen las siguientes leyes referentes a la protección de datos y la privacidad:

- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales de habeas 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.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

También el Consejo Nacional de política económica y social (CONPES) expidió en abril de 2016 el CONPES 3854, el cual define la política nacional de seguridad digital.

A nivel internacional, en mayo de 2018 entró en vigor en Reglamento General de Protección de Datos (RGPD) en la Unión Europea, el cual regula el tratamiento de los datos personales en ese conjunto de países.

2.4 ESTADO DEL ARTE

El estado del arte que en el presente documento se presenta, incorpora en su contenido los aspectos esenciales en dos aspectos, el primero de ellos, en las investigaciones nacionales; es decir con relación a la normatividad doméstica, y como segundo aspecto, las investigaciones de derecho comparado en materia internacional.

INVESTIGACIONES NACIONALES

Objetivo: Establecer si Colombia a la luz de la actual legislación puede considerarse como un país que garantiza un nivel adecuado de protección de los datos personales frente a las exigencias de la Unión Europea (Remolina Angarita, 2010).

Muestra: La legislación de protección de datos personales en Colombia.

El autor realiza una comparación entre la legislación colombiana y la regulación de protección de datos en la Unión Europea, resaltando las debilidades y fortalezas de la legislación colombiana; cabe resaltar que el estudio fue realizado en el año 2010 cuando Colombia aún no contaba con una legislación particular en materia de protección de datos personales, por tanto el nivel "adecuado" que se menciona en la regulación Europea no se cumple para la época en la que se realizó el estudio.

Resultados: La ley 1266 es una norma sectorial es decir se aplica solamente a los datos personales crediticios y financieros; no regula los datos sensibles, no consagra el derecho a la oposición, contiene disposiciones inadecuadas sobre transferencia internacional de datos personales.

Objetivo: Mostrar el panorama normativo de protección de datos personales en Colombia y su evolución frente a la sociedad de la información y las telecomunicaciones, en cumplimiento de las normas aplicables al sector privado y público y el Derecho comparado (Rojas bejarano, 2014).

Muestra: Legislación colombiana en materia de protección de datos personales.

Además del artículo 15 de la Constitución Política de Colombia, el proceso de protección de datos personales en Colombia inició con la Ley 1266 de 2008 como norma especial y luego con la expedición de la Ley 1581 de 2012, ésta última fue parcialmente reglamentada por el decreto 1377 de 2013, además se menciona los principios rectores de la protección de datos en la legislación colombiana, de igual manera se hace alusión a los tipos de datos personales que se mencionan en la Ley, transferencia internacional de datos personales.

Resultados: Latinoamérica no tiene un tratado internacional que plantee las directrices que deben cumplirse, los países latinoamericanos han hecho esfuerzos para garantizar la protección de datos mediante el reconocimiento constitucional, sin embargo existen países como Colombia, Argentina, Uruguay, Costa Rica, entre otros que lo han regulado por medio de leyes específicas.

INVESTIGACIONES INTERNACIONALES.

Objetivo: Plantear un análisis del nivel de protección de la privacidad versus la seguridad en la actual era del internet (Şerbu & Rotariu, 2015).

Muestra: Motores de búsqueda.

Actualmente se está presentando una creciente problemática en materia de intimidad en internet, debido a que la totalidad de la información se encuentra disponible en el ambiente online, debido a que la información derivada de la intimidad se utiliza para el marketing, la comunicación y estadísticas, convirtiendo en gran medida en un producto.

Por otro lado, el concepto de vida privada se aparta de las barreras físicas, debido a que la información que en principio resulta ser privada se aparta en la actualidad, con el fácil acceso de la información y en especial en temas de orientación sexual, historia clínica, y la información financiera, que bajo ningún aspecto puede ser estrictamente enmarcada en un aspecto corpóreo.

Resultados: Producto del creciente riesgo de la intimidad, según Edward Snowden, empleado de la CIA y la NSA, habló sobre las interceptaciones hechas por el Gobiernos de ciertos países, señalando que más personas usan mensajes cifrados y técnicas en línea para ocultar su historial de actividades en internet.

Con relación a los datos personales en línea, a medida que internet es testigo de un mayor desarrollo, la confianza de los consumidores es esencial para el éxito registrado en línea y sobre todo de la economía digital. Cuanto más esta confianza está aumentando el éxito será el negocio en línea. En este sentido se debe considerar la intimidad y la seguridad que debe ofrecerse a los clientes, en la misma medida, resulta muy importante encontrar una buena dirección de Internet en el futuro, y la futura generación será tomada hoy en día.

3 METODOLOGÍA

La presente investigación abarca temas concernientes al tratamiento de datos personales en

internet; cabe resaltar que las regulaciones aplicadas a este tipo de espacios virtuales no han sido abordadas en muchos ámbitos de estudio. Se evidencia que hay pocos estudios sobre el cumplimiento de la legislación colombiana en protección de datos personales en internet.

Por lo anterior, la metodología de investigación que se empleará en el presente proyecto es la exploratoria. Tal y como se dijo anteriormente, son escasos los estudios conocidos en este tema, y esta metodología permite que se brinde una visión general de la garantía del derecho a la intimidad respecto a los servicios que se prestan en internet; siendo de gran utilidad para aumentar el grado de familiaridad con temáticas relativamente desconocidas como la que se está realizando en este proyecto, y así obtener información sobre la posibilidad de realizar una investigación más completa.

3.1 FASES DEL TRABAJO DE GRADO

El presente trabajo de investigación se desarrollará en las siguientes fases:

3.1.1. Revisión de la regulación colombiana actual en cuanto a protección de datos personales.

3.1.2. Análisis de los términos y condiciones de los servicios de internet objeto de estudio.

3.1.3. Comparación y equivalencias entre los términos y condiciones de los servicios de internet objeto de estudio y la legislación colombiana vigente.

3.1.4. Presentación de resultados de cumplimientos o desviaciones de los dos aspectos analizados.

3.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Se utilizaron las Políticas de los servicios de internet definidos en el alcance del proyecto, las cuales se encuentran disponibles en sus sitios web respectivos. Adicionalmente se utilizó el servicio de geolocalización www.geoipview.com y el programa de ofimática Excel.

3.3 POBLACIÓN Y MUESTRA

A continuación se relacionan las poblaciones y muestras consideradas durante el desarrollo del proyecto.

Población 1: Regulación internacional en materia de protección de datos personales y habeas data.

Población 2: Los servicios colaborativos que se prestan en internet.

Muestra 1: Legislación colombiana en materia de protección de datos personales.

Muestra 2: Servicios de Facebook, Google, Microsoft y Twitter.

3.4 ALCANCE Y LIMITACIONES

Durante el desarrollo de este proyecto, es importante acotar los servicios de internet que serán objeto de estudio, pues actualmente existe un gran número de éstos servicios que resultaría supremamente complejo analizar en su totalidad. Por lo anterior, se define el alcance del proyecto y las limitaciones que se tienen dentro de la investigación para el estudio de los servicios de internet seleccionados.

3.4.1 ALCANCE

El alcance del presente proyecto se encuentra demarcado entre los siguientes servicios de internet gratuitos: Facebook, Twitter, servicios de Google, servicios de Microsoft; analizando el enfoque de los usuarios según los términos y condiciones de estos servicios, así mismo el uso que se le da a estos servicios de manera personal.

Este proyecto se enfoca en el estudio de la legislación colombiana en materia de protección de datos personales.

3.4.2 LIMITACIONES

La limitación de este proyecto es la imposibilidad de validar el cumplimiento de estas políticas de privacidad a nivel interno de las organizaciones que son objeto de estudio.

Este proyecto de investigación se limita a los requisitos establecidos en la legislación colombiana en temas de protección de datos personales.

4 PRODUCTOS A ENTREGAR

Los productos que este proyecto entrega son:

- Una recopilación de los tipos de datos personales que actualmente se recogen por los servicios de internet.

- Un análisis del cumplimiento de estos servicios con la legislación en materia de protección de datos en Colombia.
- Un análisis comparativo entre la legislación colombiana actual concerniente a la protección de datos con referentes internacionales en la misma materia, que permita encontrar fortalezas y debilidades en la legislación colombiana actual.

5 ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

- Conocer los puntos más críticos del cumplimiento de la legislación colombiana en los servicios de internet.
- Resaltar la importancia de una legislación alineada con la realidad mundial, en temas de protección de datos personales.
- Destacar la relevancia de tener una legislación eficaz para la protección de los datos personales en nuevos escenarios como el ciberespacio.
- Recomendaciones a los usuarios colombianos de los servicios de internet en temas de protección del derecho a la intimidad en el ciberespacio.

Resaltar la importancia de una legislación alineada con la realidad mundial, en temas de protección de datos personales.

Es conocido por muchas personas, que el siglo XXI ha traído consigo gran cantidad de cambios, tanto en la industria, el transporte, el comercio, relaciones internacionales, en fin; pero la era de internet podría ser sin lugar a duda el mayor cambio que ha llegado a la humanidad en los últimos tiempos, pues haciendo una comparación de cómo se realizaban las actividades cotidianas que llevamos a cabo hoy en día con la manera de realizarlas hace por lo menos treinta años notamos a simple vista el impacto que ha generado internet en la vida y desarrollo del ser humano; en las comunicaciones por ejemplo; hace tres décadas era necesario el envío de algún mensaje a través de los sistemas de correspondencia de la época, dependiendo completamente de los tiempos del proveedor del servicio para que la entrega del documento o comunicación fuera efectuada.

Hoy en día con el uso de las nuevas tecnologías y la masificación de las mismas, la mayoría de las personas lleva consigo un dispositivo de comunicación que permite realizar este tipo de tareas en cantidades de tiempo muy inferiores a la cantidad de tiempo gastado en los años ochenta para la misma tarea. De ahí con un ejemplo tan sencillo como el mostrado, se puede ver como internet cambiado la manera como nos comunicamos, compartimos información, aprendemos, compramos productos y servicios, surgiendo de esta manera nuevos escenarios que necesitan ser analizados con detenimiento a fin de salvaguardar la intimidad del ser humano, al abordar estos espacios hasta hace algunos años desconocidos.

Diariamente con el uso que le damos desde nuestro ámbito personal a internet exponemos cantidades considerables de información que permite revelar en gran medida lo que somos; cómo nos comportamos, nuestros gustos, los lugares que frecuentamos, nuestros medios de pago, entre otras, es decir todo nuestro paso por internet tiene su trazabilidad, ésta información normalmente es usada por los proveedores de aplicaciones en internet para poder comercializar productos o servicios de acuerdo con el perfil o preferencias de cada usuario.

De lo anterior, podemos deducir que la información de tipo personal que se procesa en internet puede identificar o hacer identificable a una persona en particular, puesto que se incluye información de tipo identificación como nombre, dirección, teléfono, fotografías; entre otras, de ahí la importancia de la protección de esa información en ámbitos intangibles como lo es internet o como es conocido hoy en día el ciberespacio.

Cada día es muy común ver como se ofrecen en internet servicios “gratuitos” como motores de búsqueda, correo electrónico, acceso a redes sociales, música, películas, servicios de entretenimiento, entre otros, ahora bien, ¿cómo se financian estos servicios si el usuario final no entrega una remuneración por su uso?, cabe resaltar una frase que se escucha muy a menudo por estos días “la era de la información”, y es bastante asertiva si la aplicamos al uso de servicios en internet sin pagar por ellos, es decir que probablemente la remuneración que se está pagando por el uso de los servicios mencionados sea la propia información del usuario, en el desarrollo de éste capítulo, se expone una consolidación de los datos personales que los servicios de internet del alcance de este proyecto recopilan para la prestación de sus respectivos servicios. A continuación se realiza una recopilación de

los tipos de datos recolectados por los servicios de internet definidos en el alcance del proyecto, basada en la información que se encuentra disponible en sus sitios web correspondientes.

La tabla 1 relaciona la información de datos personales que son recopilados por los servicios de Google, así como la naturaleza de estos.

Tabla 1 Información recopilada por los servicios de Google. Fuente: Elaboración propia.

Tipo de información	Tipo de dato
Idioma de uso	Público
Dirección IP	Privado
Cookies (Identificadores únicos)	Privado
Identificador del dispositivo	Privado
Identificador del navegador	Semiprivado
Identificador de la aplicación que se usa para conectar con Google	Semiprivado
Nombre	Público
Dirección de correo electrónico	Semiprivado
Dirección de facturación	Privado
Contraseña	Privado
Número de teléfono	Privado
Datos de pago (tarjeta de crédito)	Privado
Fecha de nacimiento	Semiprivado
Correos electrónicos enviados o recibidos	Privado
Fotos que se guardan en el almacenamiento de Google	Sensible
Videos que se guardan en el almacenamiento de Google	Sensible
Documentos, hojas de cálculo que se guardan en el almacenamiento de Google	Privado
Comentarios de Youtube	Semiprivado
Aplicaciones, navegadores y dispositivos	
Tipo de navegador y su configuración	Semiprivado
Sistema operativo	Semiprivado
Información sobre la red móvil (como el nombre del operador y el número de teléfono)	Privado
Número de versión de la aplicación	Privado
Actividad del sistema	Privado
Fecha de nacimiento	Semiprivado
Hora	Privado
URL referencia de la petición de fallo	Privado
Tipo del dispositivo	Privado
Nombre del operador	Privado

Aplicaciones instaladas	Privado
Actividad	
Los términos que busca el usuario	Privado
Los vídeos que ve el usuario	Privado
Las visualizaciones y las interacciones con el contenido y los anuncios	Privado
Información sobre voz y audio cuando utilizas funciones de audio	Privado
Actividad de compra	Privado
Usuarios con los que se comunica o comparte contenido	Privado
Actividad en sitios web y aplicaciones de terceros que utilizan nuestros servicios	Privado
Historial de navegación de Chrome que ha sincronizado con la cuenta de Google	Privado
Hangouts - Google Voice	
Número de teléfono	Privado
Número de las personas a las que llama	Privado
Número de desvío de llamadas	Privado
Fecha y hora de llamadas	Privado
Mensajes	Privado
Duración de llamadas	Privado
Información de enrutamiento	Semiprivado
Tipos de llamadas	Privado
Información de Ubicación	
GPS	Privado
Dirección IP	Privado
Datos del sensor de tu dispositivo	Privado
Información sobre elementos cercanos al dispositivo como, por ejemplo, puntos de acceso Wi-Fi, antenas de servicio de telefonía móvil y dispositivos con el Bluetooth activado	Privado
Etiquetas de píxel	Privado
Registros del servidor	Privado

Los servicios de Google se destacan porque están presentes en el sistema operativo de un gran número de teléfonos inteligentes como lo es Android, esto que puede ser un arma de doble filo para el gigante de internet, pues en día pasados fue multado por un poco más $4.300 millones de euros por abuso de posición dominante en el sistema operativo Android("Multa histórica de la UE a Google por Android: 4.340 millones de euros por abuso de posición dominante," 2018), al ser el gigante de internet, Google se respalda en su necesidad de ofrecer un servicio ubicuo, sin necesidad de estar preguntando al usuario por datos que puede ser tomados trasparentemente por sensores del teléfono, ubicación, contactos frecuentes, rutinas de transporte, es decir lo que brinda es una experiencia en el uso de sus

servicios a costa de la entrega de la cantidad de datos que relacionaron en la tabla 1.

De igual manera, Microsoft al tener gran parte del mercado mundial con sus sistemas operativos para computadoras de escritorio, portátiles, teléfonos celulares, entre otros ofrece diferentes servicios entre los que se destacan el asistente virtual Cortana y la consola de videojuegos Xbox, aún no con tanta fuerza como hace algunos años el correo electrónico de Microsoft Outlook, permite captar gran cantidad de usuarios de internet. En la tabla 2 se relaciona la información de datos personales que son recopilados por los servicios de Microsoft, de igual manera se hace una distinción de los tipos de datos recopilados.

Tabla 2 Información recopilada por los servicios de Microsoft. Fuente: Elaboración propia.

Tipo de información	Tipo de dato
Cookies	Privado
Id de publicidad	Privado
Balizas web	Privado
Credenciales	Privado
Nombre	Público
Datos de contacto	Privado
Datos de pago	Privado
Datos del dispositivo	Privado
Los contactos	Privado
Actividades	Privado
Intereses	Privado
Favoritos	Privado
Cortana	
Frecuencia cardíaca	Sensible
Pasos realizados	Privado
Datos de ubicación	Privado
Calorías	Sensible
Contactos (nombres, apellidos, nombre de la empresa donde trabaja)	Privado
Correo electrónico	Privado
Mensajes de texto	Privado
Información de llamadas entrantes y salientes	Privado
Tráfico cercano	Privado
Envío de correo electrónico en su nombre	Privado
Calendario	Privado
Historial de navegación	Privado

Micrófono	Sensible
Almacenamiento	Privado
Xbox	
Información de actividad de juego	Privado
Uso de juegos	Privado
Gamertag	Semiprivado
Puntación del jugador	Privado
Historial de juegos	Privado
Lista de amigos	Privado

Otro de los servicios más relevantes y de mayor uso que actualmente se prestan en internet son las redes sociales, la instantaneidad que presiona al ser humano del siglo XXI, hace que la hiperconexión a este tipo de tecnologías sea cada vez más creciente, el hecho de poder publicar con quién estas, qué comes, en dónde estás, es una convergencia que mezcla la necesidad del ser humano del ser aceptado con la inmediatez del momento en el que suceden los hechos; compartir en vivo un concierto en internet, es una idea que hace algunos años era imposible, hoy con uno de los servicios que ofrece Facebook y su integración con otras compañías un usuario común puede realizar estas tareas con un solo click, una vez explicadas brevemente las bondades de los servicios que se prestan en las redes sociales, se procede con la exposición del listado de tipos de datos personales que se recopilan alrededor del mundo.

La tabla 3 relaciona la información de datos personales que son recopilados por los servicios de Facebook así como la naturaleza de los mismos, mientras que la tabla 4 relaciona la información de datos personales que son recopilados por los servicios de Twitter.

Tabla 3 Información recopilada por los servicios de Facebook. Fuente: Elaboración propia.

Tipo de información	Tipo de datos
Contenido de las publicaciones	Privado
Comunicaciones	Privado
Metadatos de los contenidos subidos a Facebook	Privado
Creencias religiosas	Sensible
Ideologías políticas	Sensible
Intereses	Privado
Información de salud	Sensible
Origen étnico o racial	Sensible

Creencias filosóficas	Sensible
Afiliación sindical	Sensible
Contactos	Privado
Páginas que se conecta el usuario	Privado
Las cuentas con las que se conecta el usuario	Privado
Grupos con los que se conecta el usuario	Privado
Sincronizando el dispositivo	Privado
Libreta de direcciones	Privado
Registro de llamadas	Privado
Historial de SMS	Privado
Uso de productos de Facebook	Privado
Funciones que se utilizan	Privado
Hora, frecuencia y duración de actividades	Privado
Contenido que ve el usuario	Privado
Información de pago, como el número de la tarjeta de crédito o débito y otra información sobre la tarjeta; otra información sobre la cuenta y la autenticación; y detalles de facturación, envío y contacto.	Privado
Información del dispositivo de conexión	
Atributos del dispositivo: información como el sistema operativo, las versiones de hardware y software, el nivel de carga de la batería, la potencia de la señal, el espacio de almacenamiento disponible, el tipo de navegador, los tipos y nombres de aplicaciones y archivos, y los plugins.	Privado
Operaciones del dispositivo: información sobre las operaciones y los comportamientos realizados en el dispositivo, como poner una ventana en primer o segundo plano, o los movimientos del mouse (lo que permite distinguir a humanos de bots).	Privado
Identificadores: identificadores únicos, identificadores de dispositivos e identificadores de otro tipo, como aquellos provenientes de juegos, aplicaciones o cuentas que usas, así como identificadores de dispositivos familiares (u otros identificadores exclusivos de los Productos de las empresas de Facebook y que se vinculan con la misma cuenta o el mismo dispositivo).	Privado
Señales del dispositivo: señales de Bluetooth e información sobre puntos de acceso a wifi, balizas ("beacons") y torres de telefonía celular cercanos.	Privado
Datos de la configuración del dispositivo: información que nos permites recibir mediante la configuración que activas en tu dispositivo, como el acceso a la ubicación de GPS, la cámara o las fotos.	Privado
Red y conexiones: información, como el nombre del operador de telefonía celular o proveedor de internet, el idioma, la zona horaria, el número de teléfono celular, la dirección IP, la velocidad de la conexión y, en algunos casos, información sobre otros dispositivos que se encuentran cerca o están en tu red, para que podamos hacer cosas como ayudarte, por ejemplo, a transmitir un video del teléfono al televisor.	Privado
Datos de cookies: datos provenientes de las cookies almacenadas en tu dispositivo, incluidos la configuración y los identificadores de cookies.	Privado

Tabla 4 Información recopilada por los servicios de Twitter. Fuente: Elaboración propia.

Tipo de información	Tipo de dato
Nombre	Público
Nombre de usuario	Público
Contraseña	Privado
Correo electrónico	Privado
Cookies	Privado
Información de ubicación	Privado
Zona horaria	Público
Idioma	Público
País	Público
Interacción con enlaces en los servicios de Twitter	Privado
Términos de búsqueda e información de cookies	Privado
Información del dispositivo (incluidas las ID del aparato y de la aplicación)	Privado
Datos de pago	Privado
Tarjeta de crédito o débito	Privado
Fecha de vencimiento de la tarjeta	Privado
Código de verificación	Privado
Dirección de facturación	Privado
Tipo de navegador	Privado
Sistema operativo	Privado
Historial de navegación	Privado
Proveedor de servicios de telefonía móvil	Privado
Cookies	Privado
Fecha de nacimiento	Privado

La figura 2, evidencia de forma general, la naturaleza de los datos que cada uno de los servicios de internet recopilan. Se evidencia que de los servicios de internet del alcance de este proyecto, Google es el que más recopila datos personales, principalmente privados. Cabe hacer claridad que la gráfica compara la cantidad de datos personales por tipo de datos, lo anterior no quiere decir que los datos recopilados sean los mismos.

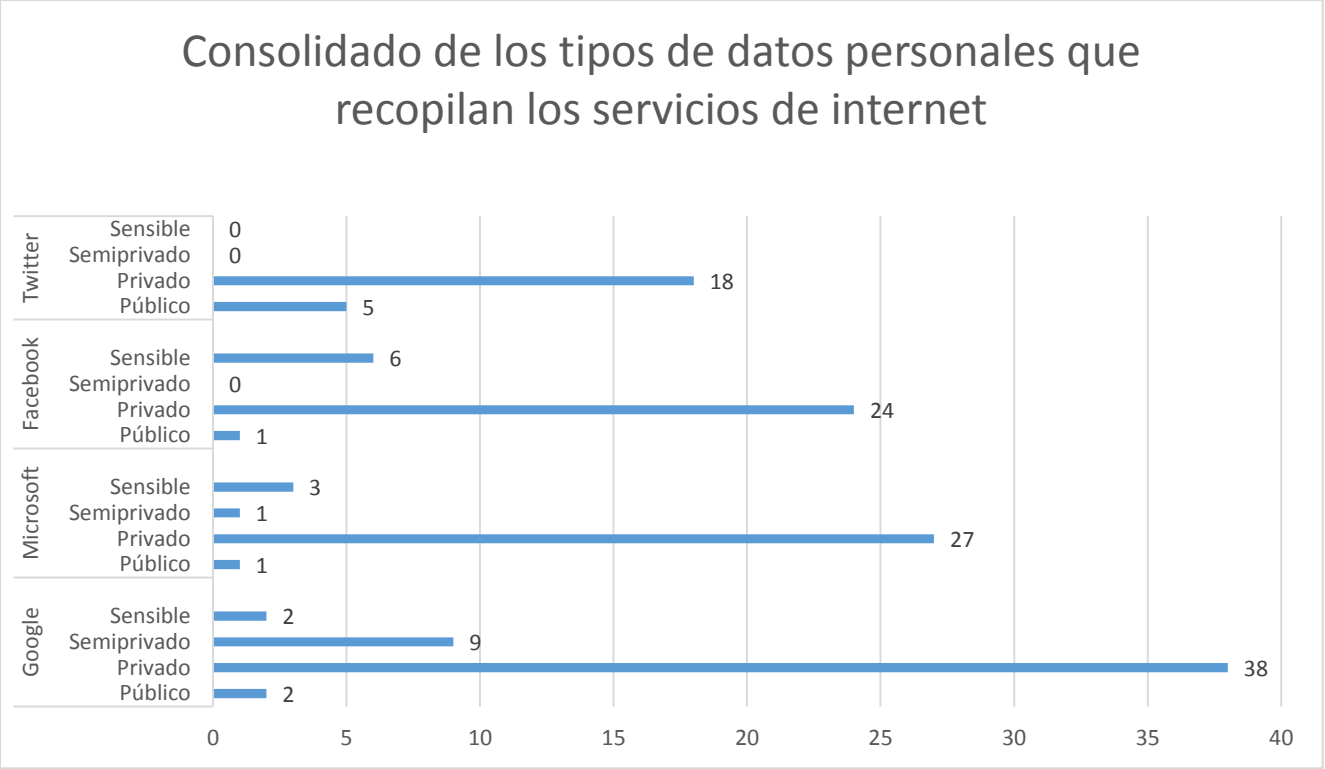

Figura 2: Consolidado de datos personales recopilados por los servicios de internet. Fuente: Elaboración propia.

De igual manera, la figura 2 muestra que la mayoría de los datos personales que son tratados en internet son privados, semiprivados y algunos sensibles.

De acuerdo con la información de datos personales identificada, se puede afirmar que los datos que se comparten a los servicios de internet son en gran medida privados dada su naturaleza, pues los servicios analizados suponen más del 50% del total de datos personales que se recopilan por cada uno de los proveedores comparados. Lo anterior resalta la importancia de contar con los controles necesarios para salvaguardar la información con el nivel de protección adecuado, de lo contrario la información de carácter personal estaría expuestas a grandes riesgos de seguridad de la información, que si no se gestionan adecuadamente acarrearían para el usuario impactos graves para su información, y más aún poner en entredicho la protección de su derecho fundamental a la intimidad.

En los siguientes capítulos se mostrará que garantías tienen los cibernautas colombianos cuando exponen su información de carácter personal a los servicios que se prestan en internet, una vez son

aceptados los términos y condiciones de los servicios.

Conocer los puntos más críticos de la legislación colombiana para destacar la relevancia de tener una legislación eficaz para la protección de los datos personales en nuevos escenarios como el ciberespacio

Una vez se han identificado los tipos de datos personales que son tratados en internet, es necesario realizar un análisis del nivel de aplicación y cumplimiento de éstos servicios de acuerdo con la normatividad colombiana, todo esto nos permite tener un panorama claro de las garantías que tienen los usuarios colombianos cuando usan los servicios de internet; o si por el contrario hay un vacío que genera una incertidumbre en la protección del derecho a la intimidad cuando se usan estos servicios.

Inicialmente se procede con la identificación del ámbito de aplicación y los requisitos de cumplimiento de la Ley de Protección de Datos Personales; mediante el Decreto 1377 de 2013 se reglamentó parcialmente la Ley 1581 de 2012 con el fin de facilitar el cumplimiento de la ley. En el artículo 2 de la Ley 1581 de 2012 se enuncia: *"La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.*(Congreso de la república, 2012)*"*; esto hace referencia a que es legislación nacional, la cual tendrá aplicación hasta los límites fronterizos. De igual manera las personas que se encuentren de paso en el territorio, deben obedecer el efectivo cumplimiento de las ley vigente al momento en que ejercer actos y configurar hechos.

En este sentido, la aplicación de las leyes objeto del presente análisis surten efectos a partir de entrada en vigor de la norma, y es aplicable dentro del territorio colombiano enmarcados en la ley y los tratados internacionales, los cuales hacen parte del bloque de constitucionalidad1, sin superar los

[1]"*La Corporación definió entonces el bloque de constitucionalidad como aquella unidad jurídica compuesta por...normas y principios que, sin aparecer formalmente en el articulado del texto constitucional, son utilizados como parámetros del control de constitucionalidad de las leyes, por cuanto han sido normativamente integrados a la Constitución, por diversas vías y por mandato de la propia Constitución. Son pues verdaderos principios y reglas de valor constitucional, esto es, son normas situadas en el nivel constitucional, a pesar de que puedan a veces contener mecanismos de reforma diversos al de las normas del articulado constitucional strictu*

límites fronterizos, puesto que esto vulneraría el principio de soberanía de los demás estados, quienes gozan de plena autonomía sobre la regulación y administración de sus ciudadanos.

En el caso de orientar esfuerzos para que cierta normatividad sea aplicable en diferentes estados, se requiere la celebración de diversos tratados internacionales, o efectuar una regulación en el marco de una unión de estados, como sucede en el caso de la unión europea, quien ha desarrollado importantes modelos regulatorios de carácter legal, que permiten dar aplicación en diversos territorios, y que a su vez configura una armonización de legislaciones.

Dicha armonización pretende la existencia de un sistema global normativo, que facilite la aplicación y la interpretación de la normatividad existente frente a las situaciones que se presentan en la dinámica social, que para el caso puntual, hace referencia al uso de información de datos personales, y sumado a ello, tras el análisis de la dinámica global de tratamiento de datos personales, se hace necesario la existencia de una normatividad armonizada y aplicable a diversos estados, la cual vaya más allá de los límites territoriales propios de cada país.

Por otro lado, resulta importante establecer que, al lograr armonizar la regulación en materia de tratamiento de datos, se configura una medida con la finalidad de evitar el fórum shopping, el cual en términos de De Valdenebro se refiere a la búsqueda de "*decisiones más o menos favorables a los intereses propios en función del foro que decida el caso, con lo que en última instancia contribuye decisivamente a la disminución del fenómeno explicado."*(de Valdenebro, 2011) , esto implica que, al existir tanta diversidad de normas, las partes que intervengan en el tratamiento de datos personales podrían realizar diversidad de actos tendientes a que sea aplicable la normatividad del país el cual tenga la norma más flexible, y que por ende se beneficie los intereses individuales.

Ahora bien, tal y como se enunció, el ámbito de aplicación de la ley hace referencia a los datos personales que sean tratados en el territorio colombiano, es decir, en el caso de los servicios prestados en internet que estamos analizando debe ser analizado dónde se lleva a cabo el tratamiento de los datos personales, por esta razón se procede con la geolocalización de cada uno de los servicios a fin de ilustrar

sensu" (Sentencia c-067 de 2003, corte constitucional de Colombia)

al lector de la ubicación geográfica del responsable del tratamiento de los datos personales para los servicios objeto de estudio. Se procede con la búsqueda de cada uno de los dominios web de los servicios estudiados en la página web geoipview.com. Como resultado, a continuación se especifican las ubicaciones geográficas de los servidores que atienden a los usuarios de los servicios de internet objeto de estudio.

De acuerdo con la búsqueda realizada se pudo verificar que la ubicación de los servicios de Google es en Mountain View una ciudad de California – Estados Unidos, tal como se muestra en la figura 3.

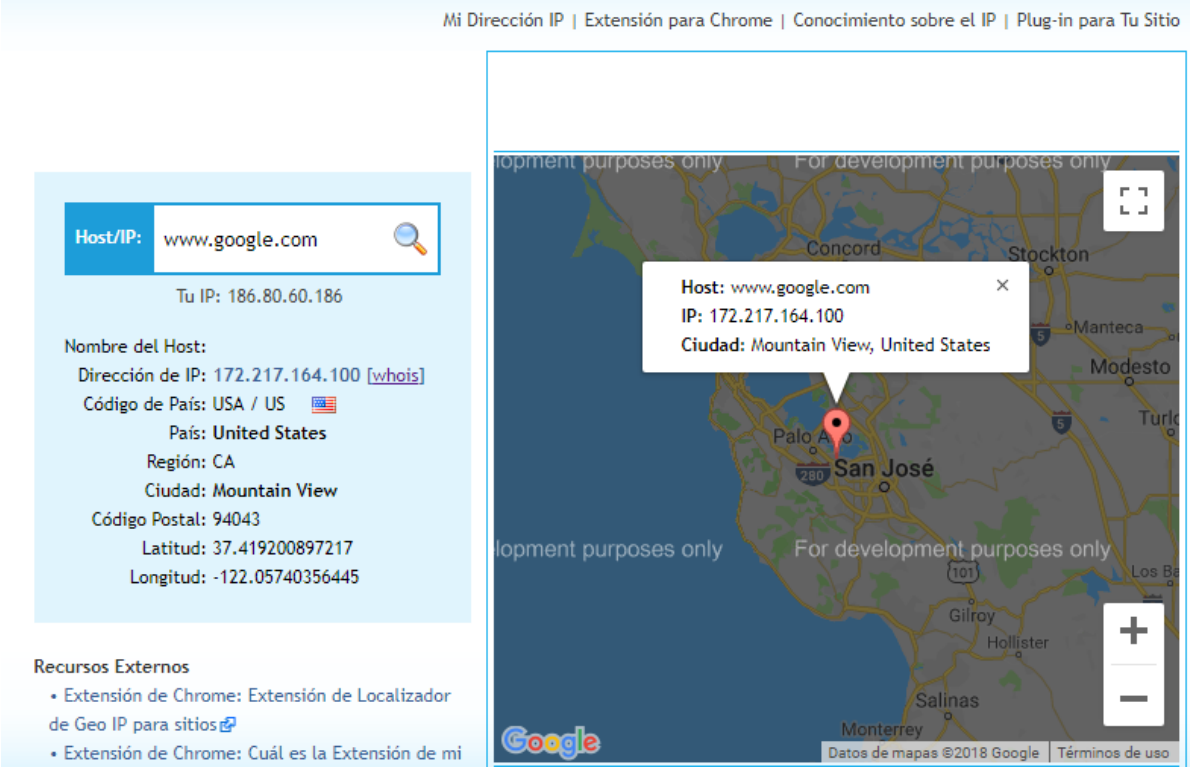

Figura 3 Geolocalización de los servicios de google. Fuente: www.geoipview.com

Respecto a los servicios de Microsoft, se pudo establecer que su ubicación es en Cambridge una ciudad de Massachusetts – Estados Unidos, tal como se muestra en la figura 4.

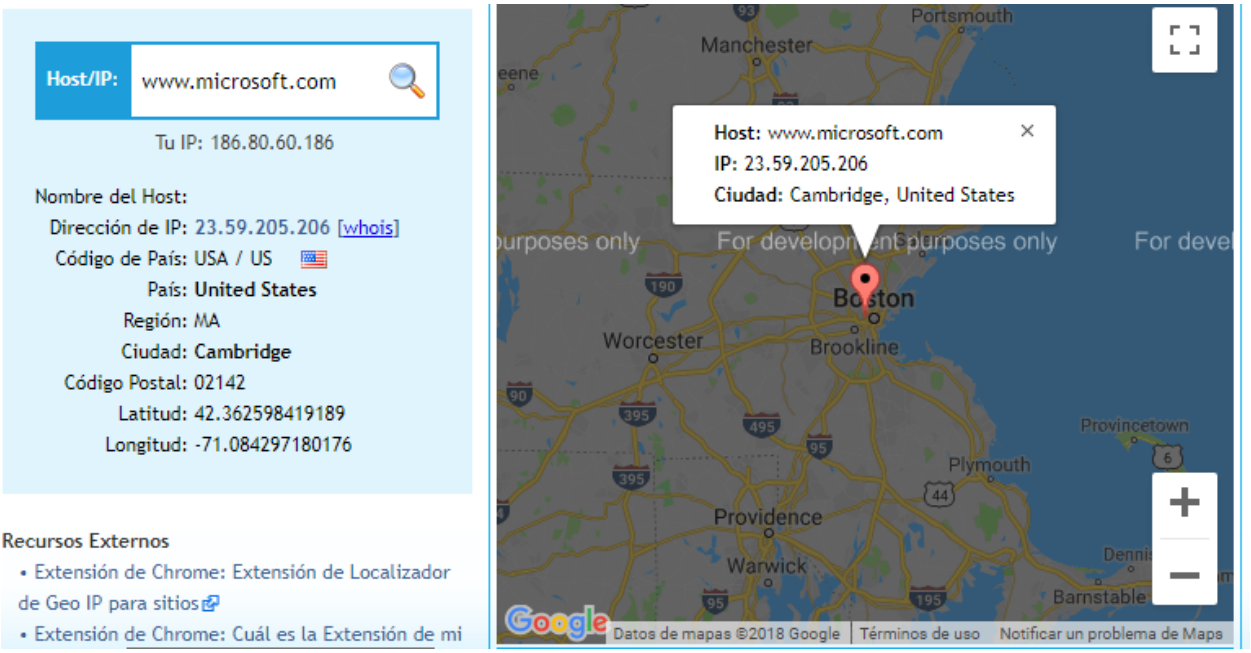

Figura 4: Geolocalización de los servicios de Microsoft. Fuente: www.geoipview.com

De acuerdo con la búsqueda realizada se pudo verificar que la ubicación de los servicios de Facebook es en Menlo Park una ciudad de California – Estados Unidos, como se evidencia en la figura 5.

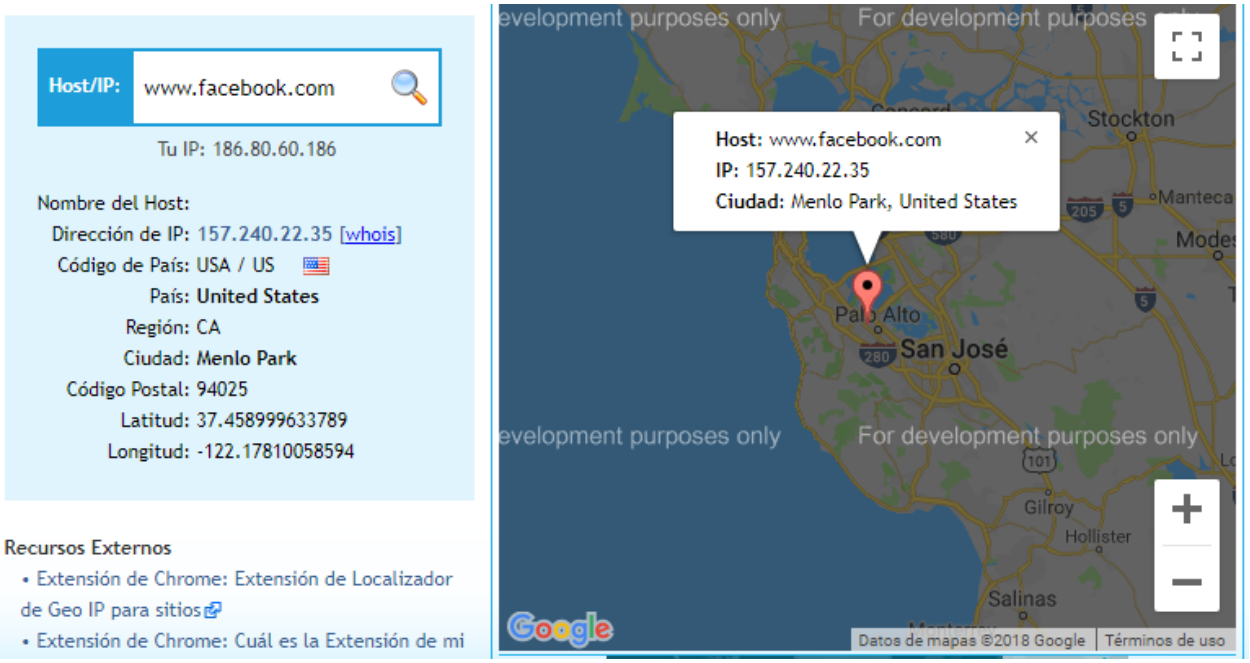

Figura 5 Geolocalización de los servicios de Facebook. Fuente: www.geoipview.com

Por último, se pudo verificar que la ubicación de los servicios de Twitter es en San Francisco una ciudad de California – Estados Unidos, tal como se muestra en la figura 6.

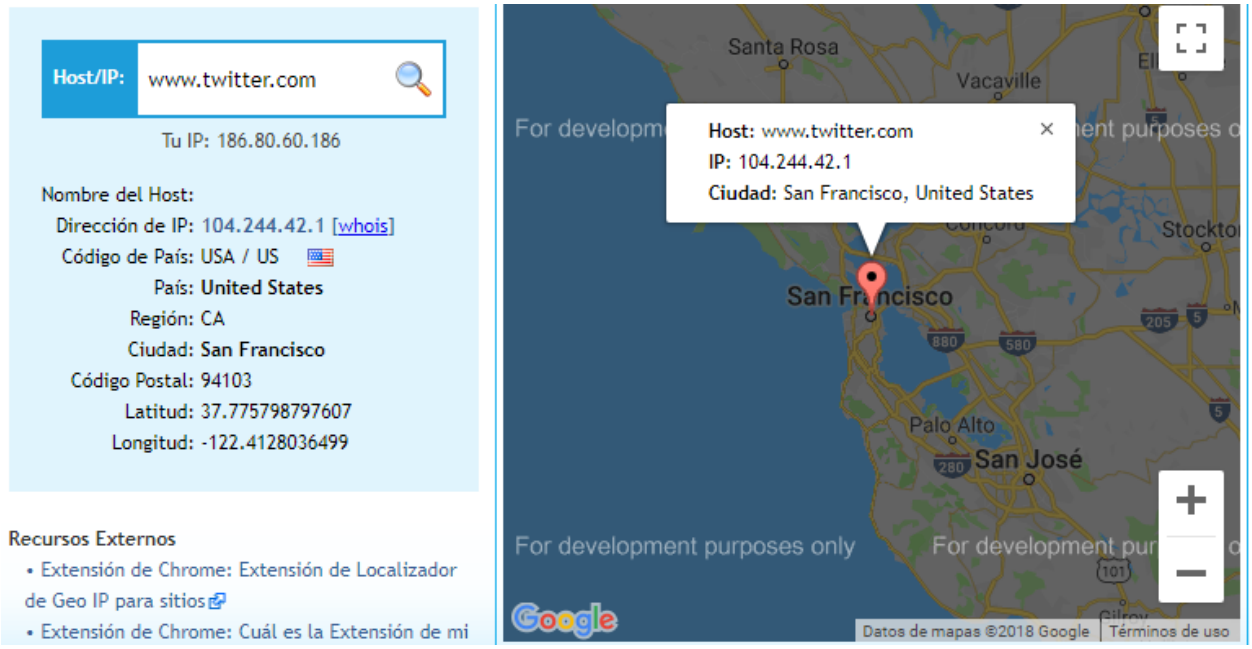

Figura 6 Geolocalización de los servicios de Twitter. Fuente: www.geoipview.com

Se pudo evidenciar que los servicios del alcance de la presente investigación están ubicados en los Estados Unidos de Norte América, por tanto, según las definiciones dadas en el artículo 2 de la Ley 1581 de 2012, esta ley no les aplica puesto que los responsables del tratamiento en este caso no están ubicados en el territorio colombiano.

Aunado a lo anterior dado que los datos personales están alojados en Estados Unidos de América, rigen las normas norteamericanas, entre todas resalta la Ley Patriota (“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” lo que traduce “Unir y Fortalecer América al Proporcionar las Herramientas necesarias para Interceptar y Obstruir el Terrorismo”) de Estados Unidos la cual fue sancionada luego de los atentados terroristas de 11 de septiembre de 2001; ésta ley tiene como fin proteger los intereses de Estados Unidos de América y fortalecer los temas de seguridad nacional, tal como data en el artículo 215 “Access to records and other items under the Foreign Intelligence Surveillance” a lo que hace referencia el artículo mencionado es que el FBI podría en cualquier momento tener acceso a los registros de las bases de datos de los operadores de servicios como los mencionados en la presente investigación, todo esto en pro de la seguridad nacional, violando de esta manera el derecho a la intimidad de los colombianos, el cual pretende ser regulado por la Ley de Protección de Datos colombiana.

Tal como se expuso en el anterior texto, la normatividad colombiana carece de fuerza de cumplimiento frente a terceras jurisdicciones en este caso Estados Unidos, todo esto puesto que no existes convenios internacionales que creen vías o instituciones que garanticen la protección de datos personales.

Sin embargo, el Congreso de la República con el ánimo de nivelar a Colombia con estándares internacionales en protección de datos, orientó la expedición de la ley en principio en un buen sentido al regular mediante el Decreto 1377 de 2013 donde se definen los requisitos para el cumplimiento de la Ley 1581 de 2012, tal como se menciona a continuación:

- Políticas de Tratamiento de los Responsables y Encargados,
- Ejercicio de los derechos de los Titulares de información
- Transferencias de datos personales
- Responsabilidad demostrada frente al Tratamiento de datos personales

Mediante las estipulaciones del mencionado decreto se puede establecer que los requisitos de cumplimiento de la ley son los siguientes:

- **Procedimientos para el tratamiento:** El responsable debe definir los procedimientos a usar para la recolección, almacenamiento, uso, circulación y supresión de información (en adelante raucs), como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.
- Autorización del titular – incluyendo la finalidad del tratamiento
- Autorización para el tratamiento de datos sensibles – en caso de requerirse el tratamiento de esos datos.
- **Mecanismos para obtener la autorización**
- **Prueba de la autorización**
- **Canales de atención:** El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión

de datos o la revocatoria de la autorización otorgada.

- **Limitación temporal del tratamiento:** Los responsables y encargados del tratamiento deberán documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate.
- **Tratamiento de datos personales de niños, niñas y adolescentes:** El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7o de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

  1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
  2. Que se asegure el respeto de sus derechos fundamentales.

  Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.
- **Políticas de tratamiento de la información:** Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento total cumplimiento a las mismas, las mismas deben contener como mínimo la siguiente información:
  - Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
  - Tratamiento al cual serán sometidos los datos y finalidad de este cuando esta no se haya informado mediante el aviso de privacidad.
  - Derechos que le asisten como Titular.
  - Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
  - Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la

autorización.

  - Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

- Aviso de privacidad: debe contener como mínimo lo siguiente:
  - Nombre o razón social y datos de contacto del responsable del tratamiento.
  - El Tratamiento al cual serán sometidos los datos y la finalidad de este.
  - Los derechos que le asisten al titular
  - Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.
- **Derechos de acceso**: El Titular podrá consultar de forma gratuita sus datos personales: (i) al menos una vez cada mes calendario y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.
- **Derecho de actualización, rectificación y supresión**: En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.
- **Medios para el ejercicio de los derechos:** Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto.

Aunque la mencionada ley no cubre los servicios del presente estudio, se realizó la evaluación de cumplimiento de los requisitos respecto de las políticas de tratamiento de datos personales con el fin de verificar la alineación de estas respecto a las disposiciones de la legislación colombiana, la tabla 5 expone los requisitos determinados en el decreto 1377 de

2013 confrontados con lo expuesto en cada una de las políticas de tratamiento de los servicios objeto de estudio; los datos fueron extraídos de las políticas de privacidad que están disponibles en cada uno de los sitios web de estos.

El color verde hace referencia que se da cumplimiento con el requisito, el color amarillo indica que cumple parcialmente, y cuando no se tiene color indica que no se encontraron datos al respecto en las políticas de tratamiento.

Tabla 5. Cumplimiento de la ley colombiana en los servicios de internet. Fuente: Elaboración propia.

Requisitos de la Ley 1581 de 2012	Google	Microsoft	Facebook	Twitter
Recolección de los datos personales: La recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente.				
• **Procedimientos para el tratamiento:** El responsable debe definir los procedimientos a usar para la recolección, almacenamiento, uso, circulación y supresión de información (en adelante raucs), como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.				
• Autorización del titular – incluyendo la finalidad del tratamiento				
• Autorización para el tratamiento de datos sensibles – en caso de requerirse el tratamiento de esos datos.				
• **Mecanismos para obtener la autorización**				
• **Prueba de la autorización**				
• **Canales de atención:** El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.				

• **Limitación temporal del tratamiento:** Los responsables y encargados del tratamiento deberán documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate				
• **Tratamiento de datos personales de niños, niñas y adolescentes:** El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7o de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:				
1. Que responda y respete el interés superior de los niños, niñas y adolescentes.				
2. Que se asegure el respeto de sus derechos fundamentales.				
• **Políticas de tratamiento de la información:** Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas, las mismas deben contener como mínimo la siguiente información:				
○ Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.				
○ Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.				
○ Derechos que le asisten como Titular.				
○ Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la				

autorización.				
○ Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.				
○ Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.				
• **Aviso de privacidad**: debe contener como mínimo lo siguiente:				
○ Nombre o razón social y datos de contacto del responsable del tratamiento.				
○ El Tratamiento al cual serán sometidos los datos y la finalidad de este.				
○ Los derechos que le asisten al titular				
○ Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.				
Medidas de seguridad: Medidas de seguridad relacionadas con el tratamiento de datos personales				
• **Derechos de acceso**: El Titular podrá consultar de forma gratuita sus datos personales: (i) al menos una vez cada mes calendario y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.				
• **Derecho de actualización, rectificación y supresión**: En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de				

datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.				
• **Medios para el ejercicio de los derechos:** Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto.				

Tal como se muestra en la tabla anterior, se puede afirmar que, del total de los servicios de internet analizados, ninguno está dando total cumplimiento a los requerimientos de la Ley 1581 de 2012.

En resumen, la normatividad colombiana en su espíritu busca la debida protección y garantía del derecho a la intimidad, sin embargo, carece de fundamento para responder a las necesidades que se derivan de la práctica internacional, enmarcados en una dinámica globalizada la cual requiere una regulación amplia y estricta y que contemple escenarios de aplicación extraterritoriales y este al nivel de la realidad mundial.

Los temas de tratamiento de datos personales, se han extendido a nivel mundial a diferentes escalas, las cuales dependen de los diversos canales y facilidades para el acceso a internet de los ciudadanos, producto de ello, la totalidad de la población se ha visto obligada a trasladar la administración de sus datos personales, en respuesta del alto uso de los mismos, comprometiendo en gran medida la privacidad de la información aportada. Por lo tanto, los países se han visto obligados a generar un marco regulatorio que garantice los derechos individuales de cada ciudadano, imponiendo diferentes mecanismos y limitación para el administrador de la información (Responsable de la información), y en beneficio del titular.

En este sentido, con los diversos marcos legales que son respuesta de las necesidades propias de cada país, cuentan con aspectos positivos y negativos, es decir, garantizar el eficaz uso de la información o, por el contrario, se pone en riesgo los derechos en materia de datos de sus ciudadanos. Por ello, se procede con la comparación de algunos marcos regulatorios que han logrado importantes avances dentro del ámbito de obligación compartida, es decir, que existe una carga para el estado de regular la debida protección de datos personales de los ciudadanos, pero también una obligación para el titular de limitar y graduar el nivel en que aporta sus datos personales.

Por tanto, se analizarán esencialmente dos marcos normativos que han sido determinantes para encuadrar grandes discusiones en materia de tratamiento de datos personales, de un lado, en América latina el tema de tratamiento de datos ha sido un tema nuevo y en creciente expansión, pero en el viejo continente, el tema de tratamiento de datos ha merecido una importante discusión y un desarrollo jurídico relevante, producto de como ya se mencionó, los grandes avances del uso de la información y de tecnologías.

El primer análisis lo merece la Declaración Universal de los Derechos Humanos, promulgada en 1948 por la Asamblea General de las Naciones Unidas, y reconocida en Colombia por medio de la ley 16 de 1972, por lo cual, en su artículo 12 la declaración garantiza que "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*"

Esto resulta ser un importante avance en materia de protección de datos personales, y da lugar a importantes discusiones para la garantía por parte de los países miembros.

Por otro lado, con la expedición del Pacto Internacional de Derechos Civiles y Políticos adoptado en 1966 por parte de Naciones Unidas, que a su vez es acogido por la legislación colombiana con la promulgación de la Ley 74 de 1968, se incorpora en el artículo 17 de dicho pacto, el cual establece:

"Artículo 17: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Por lo tanto, con estos importantes antecedentes es posible identificar las bases para el debido ejercicio y protección de los datos personales, sin embargo, esto merece mayor análisis.

Caso de la Unión Europea.

La legislación Europea ha sido un ejemplo para la mayoría de estados en el marco Europeo, por medio del denominado Reglamento general de la protección de datos (RGPD) de la Unión Europea, este último se considera ser una normatividad sólida, que responde a las actuaciones habituales de naturaleza pública o privada de los residentes o domiciliados.

En este orden de ideas, el RGPD de la UE cuenta con un ámbito de aplicación en dos aspectos, el primero de ellos en el aspecto material, y el segundo en el aspecto territorial, por lo tanto, para un debido análisis de los contenidos propios de la regulación en el marco de la unión Europea, se procede a su análisis de manera separada y puntual.

El primero de los ámbitos de aplicación versa sobre el aspecto material, el cual establece en términos del reglamento respecto de la materia la cual se trata, esto, implica que el reglamento será aplicado en el evento de que la información sea total o parcialmente administrada en determinada base datos, es decir que el reglamento interpreta que cuando el titular transfiera la administración de sus datos personales en principio el reglamento tiene aplicabilidad.

Por otro lado, el segundo aspecto a tener en cuenta, es el ámbito de aplicación territorial, el cual se relaciona en gran medida sobre la ubicación territorial de los datos personales y su administración territorial, con ello, el reglamento se entiende aplicable cuando los datos personales se encuentran siendo objeto de actividad de un establecimiento del responsable o encargado en la unión, situación que en principio no resulta ser atípica del marco regulatorio habitual, sin embargo, el reglamento hace extensible su aplicación cuando los datos sean tratados independientemente se encuentre dentro de la unión o no.

De esta manera, el reglamento establece el ámbito de aplicación para quienes residan en la unión, en los casos en que se ejerzan en calidad de oferentes, bien sea de bienes o de servicios, independientemente si el cumplimiento de la obligación de pago se hace en el territorio de la unión, o si por el contrario se ejecuta en cualquier lugar del mundo. Adicionalmente, en el control de comportamiento por parte de la soberanía del estado, el reglamento cuenta con un nivel de aplicación.

En resumen, en la unión Europea se da aplicación de normatividad aplicable a la comunidad, mediante un tratado internacional, sobre el que se puede hacer exigible el cumplimiento de la regulación expuesta.

Caso de los Estados Unidos.

El caso Norteamericano resulta ser mucho más impositivo, debido a que la regulación en su gran mayoría se orienta a garantizar el bien común en garantía de la soberanía del país, por ello, se ha flexibilizado en gran medida los derechos individuales de los ciudadanos, sean residentes o domiciliados para prevalecer asuntos de interés estatal, sectorizando de manera paulatina el marco normativo.

Caso de América Latina.

En el caso Latinoamericano, contrario al escenario Europeo no se cuenta con una regulación por vía de tratado internacional, sin embargo, en respuesta a la creciente dinámica internacional de datos personales, por parte de la Asamblea General de la OEA fue aprobada la resolución 2661 (XLI-O/11) sobre acceso a la información pública y sobre la protección de datos personales.

En términos de Remolina:

"Si la OEA adopta medidas estratégicas, beneficiará a todos los países latinoamericanos y logrará que nos convirtamos en un lugar en donde se puede invertir sin reserva en negocios que involucran transferencia de datos personales desde diversas partes del mundo. Esto hará que América Latina sea más competitiva frente a otros sitios del globo terráqueo respecto de nuevo y más

significativos en TIC e información personal" (Remolina Angarita, 2011).

En suma, el escenario latinoamericano no ha asignado la respectiva regulación en materia de tratamiento de datos personales, identificándose por ende la falta de uniformidad en la materia, y es solamente por vía legal de cada estado, donde se identificará el tratamiento propio de los datos personales de los ciudadanos.

Una vez analizados algunos aspectos relevantes derivados del marco regulatorio de la Unión europea, resulta importante establecer cuál es el nivel de obligatoriedad del estado colombiano frente al marco regulatorio de terceros estados.

El ejemplo más significativo es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE), el cual es un referente importante en cuanto a la protección de los mismos, teniendo en cuenta que su alcance aplica para los controladores o procesadores de datos cuyas sedes se encuentren dentro de alguno de los países miembros; y para organizaciones cuyas sedes se encuentren por fuera de la U.E pero que procesen datos sus residentes (Parlamento Europeo & Consejo de la Unión Europea, 2018). Teniendo en cuenta lo anterior, la tabla 6 muestra una comparación entre el Reglamento General de Protección de datos de la Unión Europea con la legislación colombiana vigente, lo que permite evidenciar algunas de las debilidades de ésta última.

Tabla 6. Reglamento General de Protección de Datos de la Unión Europea versus La ley de protección de datos personales en Colombia. Fuente: Elaboración propia.

Artículo del RGPD (Unión Europea)	**Equivalente Ley 1581 de 2012 (Colombia)**	**Observación**
Artículo 6. Licitud del tratamiento. Se definen las características que debe cumplir el tratamiento de la información para determinar si está siendo tratada de forma lícita y legal.	No se encontró equivalente.	Al no contar con la definición de características para la licitud del tratamiento, se desconocen los requisitos que debe cumplir el responsable del tratamiento de la información para este fin.
Artículo 7: Condiciones para el consentimiento. Define que el responsable del tratamiento de la información debe ser capaz de demostrar el consentimiento	No se encontró equivalente.	No se exige el consentimiento del responsable de la información para su tratamiento, lo que facilitaría el mal uso de sus datos personales

del interesado para el tratamiento de sus datos personales.		por terceros.
Artículo 10: Tratamiento de datos personales relativos a condenas e infracciones penales.	No se encontró equivalente.	La información relacionada a condenas e infracciones penales no tiene un tratamiento especial, lo cual debería ser así por tratarse de violaciones a la ley que pueden poner en riesgo la vida de los ciudadanos.
Artículo 21: Derecho a la oposición. Menciona el derecho del interesado o titular de la información a oponerse al tratamiento de su información cuando por alguna situación particular así lo requiera.	Artículo 15: Reclamos.	En la legislación colombiana no se menciona explícitamente el derecho a la oposición o su equivalente; sin embargo en el artículo 15 de la Ley 1581 de 2012 se describe el procedimiento para que el titular de la información presente reclamos al responsable del tratamiento, cuando los datos sean susceptibles a corrección, actualización o supresión.
Artículo 30: Registro de las actividades de tratamiento. Los responsables del tratamiento de la información deben llevar registro de las actividades de tratamiento de la información que tengan bajo su custodia.	No se encontró equivalente.	El registro de las actividades de tratamiento facilita al responsable de la información llevar el control de la misma y de igual forma supervisar cualquier evento indeseado.
Artículo 42: Certificación. Los Estados miembros de la Unión Europea deben promover la creación de mecanismos de certificación del RGPD, es decir, mecanismos que permitan certificar la protección y tratamiento de datos personales; sin embargo se aclara que la certificación será voluntaria.	No se encontró equivalente.	En Colombia no se promueve la creación de un organismo de certificación en la ley 1581 de 2012, por consiguiente tampoco existe una entidad o mecanismo que la realice. Un organismo de certificación brinda garantías al interesado de que el responsable del tratamiento de la información cumple con la legislación vigente.
Artículo 82: Derecho a la indemnización y responsabilidad. Toda persona	No se encontró equivalente.	En Colombia no existe esta figura. El artículo 23 de la Ley de Protección de datos en

que haya sufrido daños o perjuicios materiales o inmateriales como consecuencia de una infracción del responsable del tratamiento de su información, tiene derecho a una indemnización.		Colombia (1581 de 2012), menciona la facultad que tiene la Superintendencia de Industria y Comercio (SIC) para imponer sanciones a los responsables del tratamiento de datos personales; sin embargo no se mencionan indemnizaciones para el titular o interesado directamente afectado.

Teniendo en cuenta la relevancia económica y social de los países miembros de la Unión Europea, el RGPD es una guía importante para encontrar posibles mejoras o recomendaciones a la legislación colombiana actual, y así optimizar la protección de datos personales de los ciudadanos así como su derecho a la intimidad. Los artículos mencionados en la tabla 6 dan cuenta de las debilidades de las leyes colombianas con respecto a la protección de datos personales. Sin embargo, al analizar la legislación colombiana comparándola con el RGPD, también es posible encontrar muchas fortalezas entre las que se destacan la definición de un ente de vigilancia y control (Superintendencia de Industria y Comercio – SIC), la definición de principios para la protección de datos personales, los derechos de los niños y adolescentes y procedimientos para reclamos por parte de los titulares a los responsables del tratamiento.

Dado que se evidencian algunas falencias en la legislación colombiana en cuanto a la protección de datos personales, es importante realizar recomendaciones a los ciudadanos para salvaguardar la confidencialidad, integridad y disponibilidad de su información cuando voluntariamente la transfieren a los servicios de internet que se encuentran en el alcance del desarrollo de este proyecto.

Recomendaciones a los usuarios colombianos de los servicios de internet en temas de protección del derecho a la intimidad en el ciberespacio.

Una vez identificadas las debilidades y fortalezas de la legislación colombiana en el ámbito de la protección de datos, es importante sugerir a los usuarios de los servicios de internet objeto de estudio algunas recomendaciones para optimizar la confidencialidad, integridad y disponibilidad de su información en internet. Sahmin y Gharsellaoui (2017) definieron algunos problemas de seguridad y privacidad para el internet de las cosas y la computación en la nube; dado que los usuarios acceden a los

servicios de internet objeto de estudio a través de este medio, es posible sugerir los métodos técnicos y metodológicos que exponen los autores para salvaguardar la información de los usuarios con respecto a la triada de la información (Confidencialidad, integridad y disponibilidad).

Entre estos métodos se destacan:

- Cifrado: Garantiza la confidencialidad de los datos utilizando una solución criptográfica para tal fin. El cifrado de información podría aplicarse por ejemplo para las contraseñas utilizadas para acceder a los servicios.
- Ofuscamiento: Es un proceso de difusión de datos confidenciales antes de enviarlos al destino utilizando una clave secreta o método desconocido para el proveedor del servicio. Podría utilizarse por ejemplo para el envío de correos electrónicos a través del servicio de Gmail, el cual es propiedad de Google.
- Anonimización: Consiste en eliminar la información de identificación personal del registro de datos antes de enviarlo al proveedor de servicios en la nube para luego procesar con datos reales y preservar la privacidad del titular de la información. Este método garantiza la confidencialidad e integridad de la información. Se sugiere no subir información en la que se revelen datos personales privados, semiprivados o sensibles a estos servicios; en caso de ser necesario enviar información se recomienda tachar la información sensible y entregarla por otro medio.
- Segmentación de datos: Consiste en almacenar diferentes segmentos de datos separadamente. Esta metodología podría aplicarse, por ejemplo, para el envío de información personal a través de correo electrónico.
- Mediador de confianza: Es un tercero entre el usuario y el proveedor de servicios de internet que garantiza el cumplimiento de cierta política a través de la realización de auditoría.
- Gestión de claves: Es un medio para manejar las claves cifradas. Siendo la confidencialidad uno de los principales objetivos de la seguridad, el cifrado es la principal solución para obtener una óptima confidencialidad. Gestión de claves también puede entenderse como métodos básicos para tener una contraseña segura; como lo son definir una contraseña con una longitud determinada, que incluya caracteres especiales; también se sugiere no guardar contraseñas personales en los servicios de internet gratuitos.

Si bien para el usuario promedio de los servicios de internet los métodos anteriormente mencionados son desconocidos e incluso son definiciones que podrían resultar complejas de entender, el fin es no centrarse en los métodos que podrían resultar demasiado técnicos o que requieren un conocimiento avanzado en conceptos de seguridad; sino concientizar sobre el uso de los métodos básicos como por ejemplo el ofuscamiento de información o la gestión de claves. De igual manera, un usuario que tenga algunos conocimientos sobre seguridad de la información podría utilizar tanto los métodos técnicos y metodológicos para asegurar la confidencialidad, integridad y disponibilidad de su información.

Ahora bien, todo el estudio realizado fue basado en el precepto que se accede gratuitamente a los servicios de internet objeto del alcance, cabe destacar que cuando se pague por estos servicios, las políticas de privacidad y los términos y condiciones del servicio varían.

5.1 APORTE DE LOS RESULTADOS A LA EN SEGURIDAD DE LA INFORMACIÓN

Una vez conocida la situación actual y el nivel de protección que brinda la legislación colombiana a los datos que los ciudadanos colombianos exponen en el ciberespacio, se logró evidenciar la falta de protección que tienen los datos personales en estos servicios, puesto que no se está preservando de manera idónea la confidencialidad de la información o dicho de otra manera a nivel legislativo no se está protegiendo el derecho a la intimidad en el ciberespacio, es decir cuando un usuario accede a estos servicios “gratuitos” acepta todas las condiciones que le impone el prestador del servicio so pena de no poder acceder al mismo.

Los aportes que realiza este trabajo de investigación a la seguridad de la información están encaminados a mostrar las debilidades que tiene Colombia en el tratamiento de datos personales en los servicios de internet analizados así como generar recomendaciones para los usuarios finales con el fin de aumentar el grado de conciencia en el cuidado de su información personal ya que jurídicamente en este momento no se está cubriendo, en el caso colombiano.

5.2 CÓMO RESPONDE A LA PREGUNTA DE INVESTIGACIÓN CON LOS RESULTADOS

Se evidenció que si bien Colombia ha mostrado preocupación por salvaguardar los datos personales de sus ciudadanos con la expedición de leyes para tal fin, éstas presentan algunas debilidades en comparación con el reglamento europeo, el cual es un importante referente a nivel mundial. Respondiendo a la pregunta de investigación, es posible afirmar que pese al avance que ha tenido Colombia en protección de datos personales, la normatividad no es eficaz en la protección del tratamiento de datos personales en el ciberespacio. A esta respuesta se llega después del análisis realizado en comparación con la normatividad europea y después de evidenciar que en Colombia no hay un nivel de protección de datos adecuado en internet.

5.3 ESTRATEGIAS DE COMUNICACIÓN Y DIVULGACIÓN

El presente proyecto de investigación se divulgará a través de una socialización frente a los jurados asignados para tal fin, y se encontrará disponible en el repositorio de la biblioteca de la Universidad Católica de Colombia.

6. CONCLUSIONES

El presente documento tuvo como objeto construir un análisis de la procedencia y efectividad del marco regulatorio del tratamiento de datos a la luz de legislación colombiana, en respuesta de las crecientes dinámicas nacionales e internacionales en la materia, y producto de la importante necesidad de un marco regulatorio que atienda la diversidad de situaciones que se presentan en un marco globalizado, con lo cual se logró identificar algunos defectos sustanciales sobre lo siguiente:

6.1. Se formuló una identificación e individualización expresa de los tipos de datos personales almacenados por los servicios de internet planteados como objeto de estudio, logrando en esta medida identificar que el servicio que mayor información administra es Google, con 51 sobre datos principalmente privados, seguido constituyen ser Microsoft, Facebook y Twitter con 32, 31 y 23 datos personales respectivamente.

6.2. Se efectuó un análisis comparativo sobre los servicios de internet, y su nivel de cumplimiento con relación al marco regulatorio existente, concluyendo que en esta medida la legislación colombiana sólo tiene cubrimiento en el territorio colombiano, por tanto no se

cubren los servicios analizados, sin embargo se analizó el cumplimiento de los demás requisitos de ley encontrando que ningún servicio analizado cumple plenamente, constituyendo por ende una necesidad de re evaluar el ámbito de aplicación actual de la ley en materia de tratamiento de datos.

6.3. Se encontraron las debilidades y fortalezas de la legislación colombiana en materia de protección de datos personales, haciendo un análisis comparativo frente a normas internacionales y el Reglamento Europeo de Protección de Datos, siendo éste un gran referente a nivel mundial en la materia. Algunas debilidades tienen que ver con la inexistencia de un mecanismo de certificación que garantice que las organizaciones responsables del tratamiento de información estén cumpliendo con la legislación correspondiente; la no indemnización cuando el responsable del tratamiento de la información ha incurrido en alguna infracción, entre otros. Sin embargo, se encontraron también algunas fortalezas en la legislación colombiana con respecto a la internacional, entre las que se destacan la definición del tratamiento de información de niños y adolescentes y la definición de los principios de la protección de datos.
6.4. Se logró mostrar la necesidad de autocuidado que deben tener los ciudadanos colombianos cuando usan estos servicios de internet puesto que jurídicamente no se está logrando el nivel de protección requerido en escenarios como el ciberespacio.
6.5. Se logró determinar la ausencia de un tratado internacional que fije los parámetros en materia de protección de datos, y por lo tanto, en respuesta a esta omisión internacional, los países han regulado de manera separada la garantía de protección por vía legal.

7. BIBLIOGRAFÍA

Características de la geolocalización Online. (2017). Retrieved August 20, 2011, from http://reader.digitalbooks.pro/book/preview/43053/id_ch_4

Cheng, F. C., & Lai, W. H. (2012). The impact of cloud computing technology on legal infrastructure within Internet - Focusing on the protection of information privacy. *Procedia Engineering*, *29*, 241–251. https://doi.org/10.1016/j.proeng.2011.12.701

Circular externa No. 002 de 2018. (n.d.). Retrieved from http://www.sic.gov.co/sites/default/files/normatividad/032018/CIRCULAR-EXTERNA-002.pdf

Congreso de la república. (2008). Ley estatutaria 1266 del 31 de diciembre de 2008. Retrieved from http://www.sic.gov.co/recursos_user/documentos/normatividad/Leyes/2008/Ley_1266_2008.pdf

Congreso de la república. (2012). Ley 1581 de Octubre de 2012.

CONPES. (2016). Política Nacional de Seguridad Digital, 91. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ�micos/3854.pdf

de Valdenebro, J. (2011). Reflexiones sobre la unificación de Civil y comercial. La CISG como criterio aconsejable. *Revista de Derecho Privado*, 1–52. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=65162845&lang=es&site=ehost-live

Diferencias entre transmisión y transferencia de datos personales. (2017). Retrieved from https://escueladeprivacidad.com/diferencias-entre-transmision-y-transferencia-de-datos-personales/

Edgar, T. W., & Manz, D. O. (2017). *Research Methods for Cyber Security*.

Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer Law and Security Review*, *34*, 1039–1052. https://doi.org/10.1016/j.clsr.2018.04.007

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, *145*, 7. https://doi.org/10.1136/emj.2010.096966

Moreno Muñoz, M. (2014). La tensión entre privacidad y seguridad en el desarrollo de internet. *Dilemata*, (15), 181–193. Retrieved from http://dialnet.unirioja.es/servlet/articulo?codigo=4834529&info=resumen&idioma=SPA

Multa histórica de la UE a Google por Android: 4.340 millones de euros por abuso de posición dominante. (2018). Retrieved from https://www.xataka.com/moviles/multa-historica-ue-google-android-4-340-millones-euros-abuso-posicion-dominante

Parlamento Europeo, & Consejo de la Unión Europea. (2018). Reglamento europeo de protección de datos.

Pazos Castro, R. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales,¿ una relación imposible? - LEÍDO. *InDret*, *2014*(1), 18–50. Retrieved from http://www.raco.cat/index.php/InDret/article/viewFile/293053/381561

Políticas de tratamiento de la información personal en la superintendencia de industria y comercio. (2014). Retrieved from http://www.sic.gov.co/sites/default/files/files/Politicas_Habeas_Data_0.pdf

Remolina Angarita, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *Revista Colombiana de Derecho Internacional*, *16*(International Law), 489–524.

Remolina Angarita, N. (2011). Retos de la OEA en materia de protección de datos personales, 1–2.

Remolina Angarita, N., & Zuluaga Alvarez, L. F. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada — accountability — en las transferencias internacionales de datos personales Recomendaciones para los países latinoamericanos*.

Rojas bejarano, M. (2014). Evolución del Derecho de Protección de Datos personales en Colombia respecto a estándares internacionales. *Novomus Jus*, *8*, 107–139.

Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. *Procedia Computer Science*, *112*, 1516–1522. https://doi.org/10.1016/j.procs.2017.08.050

Şerbu, R., & Rotariu, I. (2015). Privacy Versus Security in the Internet Era. *Procedia Economics and Finance*, *27*(15), 73–76. https://doi.org/10.1016/S2212-5671(15)00974-0

Superintendencia de industria y comercio. (2014). Protección de datos personales: Aspectos prácticos sobre el derecho de Hábeas data. Retrieved from http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf

The Centre for Information Policy Leadership. (2009). Data Protection Accountability: The Essential Elements, (October), 21. Retrieved from http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

Transferencia internacional de datos. (n.d.). Retrieved from http://www.sic.gov.co/sites/default/files/normatividad/072017/Transferencia-internacional-de-datos-PFR2.pdf